Cohen and Thorne *Research in Number Theory* (2016) 2:29
DOI 10.1186/s40993-015-0001-y

Research in Number Theory
a SpringerOpen Journal

RESEARCH ARTICLE Open Access

Dirichlet series associated to quartic fields with given cubic resolvent

Henri Cohen[1] and Frank Thorne[2*]

*Correspondence:
thorne@math.sc.edu
[2]Department of Mathematics, University of South Carolina, 1523 Greene Street, Columbia, SC 29208, USA
Full list of author information is available at the end of the article

Abstract

Let k be a cubic field. We give an explicit formula for the Dirichlet series $\sum_K |\mathrm{Disc}(K)|^{-s}$, where the sum is over isomorphism classes of all quartic fields whose cubic resolvent field is isomorphic to k. Our work is a sequel to the unpublished preprint [12] whose results have been summarized in [7], so we include complete proofs so as not to rely on unpublished work.

This is a companion paper to [14] where we compute the Dirichlet series associated to cubic fields having a given quadratic resolvent.

2010 Mathematics Subject Classification: 11R16

1 Background

In a previous paper [14], we studied the problem of enumerating cubic fields[1] with fixed quadratic resolvent. A classical result of Cohn [16] is that

$$\sum_{K \text{cyclic cubic}} \frac{1}{\mathrm{Disc}(K)^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{1}{3^{4s}}\right) \prod_{p \equiv 1 \pmod 6} \left(1 + \frac{2}{p^{2s}}\right). \tag{1.1}$$

We generalized this as follows. If K is a non-cyclic cubic field, then its Galois closure $\widetilde{K}$ contains a unique quadratic field k, called the *quadratic resolvent*. We have $\mathrm{Disc}(K) = \mathrm{Disc}(k) f(K)^2$ for a positive integer $f(K)$, and for each fixed k we proved explicit formulas for the Dirichlet series $\sum_K f(K)^{-s}$, where the sum is over all cubic fields K with quadratic resolvent k. For example, if $k = \mathbb{Q}(\sqrt{-255})$ we have

$$\sum_K \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^s} + \frac{6}{3^{2s}}\right) \prod_{\left(\frac{6885}{p}\right)=1} \left(1 + \frac{2}{p^s}\right) + \left(1 - \frac{1}{3^s}\right) \prod_p \left(1 + \frac{\omega_L(p)}{p^s}\right), \tag{1.2}$$

where the sum is over all cubic fields with quadratic resolvent k, L is the cubic field of discriminant $6885 = (-27)\cdot(-255)$ determined by $x^3 - 12x - 1 = 0$, and $\omega_L(p)$ is equal to 2 or -1 when p is totally split or inert in L respectively, and $\omega_L(p) = 0$ otherwise. In general, the sum has a main term plus one additional term for each cubic field of discriminant $-D/3$, $-3D$, or $-27D$, where D is the discriminant of k.

Our work extended work of the first author and Morra [13], which established more general formulas in a less explicit form. In the quartic case, such formulas have been

[1]Note that in this paper, number fields are always considered up to isomorphism.

proved by the first author, Diaz y Diaz, and Olivier [7-10,12]. This work also yields explicit Dirichlet series similar to (1.1) and (1.2). For example, for any *abelian* group G set

$$\Phi(G,s)=\sum_{\mathrm{Gal}(K/\mathbb{Q})\simeq G}\frac{1}{|\mathrm{Disc}(K)|^s}\,. \tag{1.3}$$

Then we have the explicit Dirichlet series

$$\Phi(C_2,s)=\left(1-\frac{1}{2^s}+\frac{2}{2^{2s}}\right)\frac{\zeta(s)}{\zeta(2s)}-1\,,$$

$$\Phi(C_4,s)=\frac{\zeta(2s)}{2\zeta(4s)}\left(\left(1-\frac{1}{2^{2s}}+\frac{2}{2^{4s}}+\frac{4}{2^{11s}+2^{9s}}\right)\prod_{p\equiv 1 \pmod 4}\left(1+\frac{2}{p^{3s}+p^s}\right)-\left(1-\frac{1}{2^{2s}}+\frac{2}{2^{4s}}\right)\right)\,,$$

$$\Phi(V_4,s)=\frac{1}{6}\left(1+\frac{3}{2^{4s}}+\frac{6}{2^{6s}}+\frac{6}{2^{8s}}\right)\prod_{p\neq 2}\left(1+\frac{3}{p^{2s}}\right)-\frac{1}{2}\Phi(C_2,2s)-\frac{1}{6}\,.$$

The same authors proved similar formulas for those C_4 and V_4 extensions having a fixed quadratic subfield; the former is Theorem 4.3 of [8] and the latter is unpublished. They also obtained analogous formulas for D_4 extensions, for which we refer to [9] and Section 7.1 of [11]. One may also see Wright [30] and Wood [28] for some related results on general abelian extensions.

In the present paper we tackle this problem for A_4 and S_4-quartic fields. We count such fields by their *cubic resolvents*: Suppose that $K/\mathbb{Q}$ is a quartic field whose Galois closure $\widetilde{K}$ has Galois group A_4 or S_4. In the A_4 case, $\widetilde{K}$ contains a unique cyclic cubic subfield k, and in the S_4 case, $\widetilde{K}$ contains three isomorphic noncyclic cubic subfields k. In either case k is called the *cubic resolvent* of K, it is unique up to isomorphism, and it satisfies $\mathrm{Disc}(K)=\mathrm{Disc}(k)f(K)^2$ for some integer $f(K)$.

Let $\mathcal{F}(k)$ be the set of all A_4 or S_4-quartic fields whose cubic resolvent is isomorphic to k. We set the following definition.

Definition 1.1. For a cubic field k, we set

$$\Phi_k(s)=\frac{1}{a(k)}+\sum_{K\in\mathcal{F}(k)}\frac{1}{f(K)^s}\,,$$

where $a(k)=3$ if k is cyclic and $a(k)=1$ otherwise.[2]

We will prove explicit formulas for $\Phi_k(s)$, building on previous work of the first author, Diaz y Diaz, and Olivier ([12]; see also [7] for a published summary) which, like the subsequent paper [13], established a more general but less explicit formula. Since [12] is unpublished, we will include complete proofs of the results we need.

In the cubic case, our formulas involved sums over cubic fields of discriminant $-D/3$, $-3D$, and $-27D$, and in the quartic case we will sum over fields in a similar set $\mathcal{L}_2(k)$:

[2] This differs slightly from the definition given in [7].

Definition 1.2. Given any cubic field k (cyclic or not), let $\mathcal{L}(k)$ be the set of isomorphism classes of quartic fields whose cubic resolvent is isomorphic to k, with the additional restriction that the quartic is totally real when k is such. Furthermore, for any n define $\mathcal{L}(k,n^2)$ to be the subset of $\mathcal{L}(k)$ of those fields with discriminant equal to $n^2\mathrm{Disc}(k)$.

Finally, we define $\mathcal{L}_{tr}(k,64)$ to be the subset of those $L \in \mathcal{L}(k,64)$ such that 2 is totally ramified in L, and we set

$$\mathcal{L}_2(k) = \mathcal{L}(k,1) \cup \mathcal{L}(k,4) \cup \mathcal{L}(k,16) \cup \mathcal{L}_{tr}(k,64) .$$

Note that if k is totally real the elements of $\mathcal{F}(k)$ are totally real or totally complex, and $\mathcal{L}(k)$ is the subset of totally real ones, while if k is complex then the elements of $\mathcal{L}(k) = \mathcal{F}(k)$ have mixed signature $r_1 = 2, r_2 = 1$.

Remark. In this paper, quartic fields with cubic resolvent k will be denoted K or L. Generally K will refer to fields enumerated by $\Phi_k(s)$, and L will refer to fields in $\mathcal{L}_2(k)$. Note however that in many places this distinction will be irrelevant.

We introduce some standard notation for splitting types of primes in a number field. If L is, say, a quartic field, and p is a prime for which $(p) = \mathfrak{p}_1^2\mathfrak{p}_2$ in L, where $\mathfrak{p}_i$ has residue class degree i for $i = 1,2$, we say that p has splitting type (21^2) in L (or simply that p is (21^2) in L). Other splitting types such as (22), (1111), (1^4), etc. are defined similarly. Moreover, when 2 has type (1^21) in a cubic field k, we say that 2 has type $(1^21)_0$ or $(1^21)_4$ depending on whether $\mathrm{Disc}(k) \equiv 0 \pmod 8$ or $\mathrm{Disc}(k) \equiv 4 \pmod 8$.

Definition 1.3. Let L be a quartic A_4 or S_4-quartic field. For a prime number p we set

$$\omega_L(p) = \begin{cases} -1 & \text{if } p \text{ is } (4),(22), \text{ or } (21^2) \text{ in } L , \\ 1 & \text{if } p \text{ is } (211) \text{ or } (1^211) \text{ in } L , \\ 3 & \text{if } p \text{ is } (1111) \text{ in } L , \\ 0 & \text{otherwise} . \end{cases}$$

Our main theorems are the following:

Theorem 1.4. *(1) If k is any cubic field, we have*

$$2^{r_2(k)}\Phi_k(s) = \frac{1}{a(k)}M_1(s) \prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2,\, p\neq 2}\left(1+\frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k=\mathfrak{p}_1^2\mathfrak{p}_2,\, p\neq 2}\left(1+\frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\, p\neq 2}\left(1+\frac{3}{p^s}\right) + \sum_{L\in\mathcal{L}_2(k)} M_{2,L}(s) \prod_{p\neq 2}\left(1+\frac{\omega_L(p)}{p^s}\right) ,$$

where the 2-Euler factors $M_1(s)$ and $M_{2,L}(s)$ are given in the tables below, where the k and L-splits refer to the splitting of the prime 2.

(2) If k is any cyclic cubic field, we have

$$\Phi_k(s) = \frac{1}{3}M_1(s) \prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\, p\neq 2}\left(1+\frac{3}{p^s}\right) + \sum_{L\in\mathcal{L}(k,1)} M_{2,L}(s) \prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\, p\neq 2}\left(1+\frac{\omega_L(p)}{p^s}\right). \tag{1.4}$$

k-split	$M_1(s)$	$8M_1(1)$
(3)	$1+3/2^{3s}$	11
(21)	$1+1/2^{2s}+4/2^{3s}+2/2^{4s}$	15
(111)	$1+3/2^{2s}+6/2^{3s}+6/2^{4s}$	23
$(1^21)_0$	$1+1/2^{s}+2/2^{3s}+4/2^{4s}$	16
$(1^21)_4$	$1+1/2^{s}+2/2^{2s}+4/2^{4s}$	18
(1^3)	$1+1/2^{s}+2/2^{3s}$	14

k-split	L-split	n^2	$M_{2,L}(s)$, $L\in\mathcal{L}(k,n^2)$	k-split	L-split	n^2	$M_{2,L}(s)$, $L\in\mathcal{L}(k,n^2)$
(3)	(31)	1	$1+3/2^{3s}$	$(1^21)_0$	(21^2)	1	$1+1/2^{s}+2/2^{3s}-4/2^{4s}$
(3)	(1^4)	64	$1-1/2^{3s}$	$(1^21)_0$	(1^211)	1	$1+1/2^{s}+2/2^{3s}+4/2^{4s}$
(21)	(4)	1	$1+1/2^{2s}-2/2^{4s}$	$(1^21)_0$	(1^21^2)	4	$1+1/2^{s}-2/2^{3s}$
(21)	(211)	1	$1+1/2^{2s}+4/2^{3s}+2/2^{4s}$	$(1^21)_0$	(1^4)	64	$1-1/2^{s}$
(21)	(2^2)	16	$1+1/2^{2s}-4/2^{3s}+2/2^{4s}$	$(1^21)_4$	(21^2)	1	$1+1/2^{s}+2/2^{2s}-4/2^{4s}$
(21)	(1^21^2)	16	$1+1/2^{2s}-2/2^{4s}$	$(1^21)_4$	(1^211)	1	$1+1/2^{s}+2/2^{2s}+4/2^{4s}$
(21)	(1^4)	64	$1-1/2^{2s}$	$(1^21)_4$	(2^2)	4	$1+1/2^{s}-2/2^{2s}$
(111)	(22)	1	$1+3/2^{2s}-2/2^{3s}-2/2^{4s}$	$(1^21)_4$	(2^2)	16	$1-1/2^{s}$
(111)	(2^2)	16	$1-1/2^{2s}-2/2^{3s}+2/2^{4s}$	$(1^21)_4$	(1^21^2)	16	$1-1/2^{s}$
(111)	(1111)	1	$1+3/2^{2s}+6/2^{3s}+6/2^{4s}$	(1^3)	(1^31)	1	$1+1/2^{s}+2/2^{3s}$
(111)	(1^21^2)	16	$1-1/2^{2s}+2/2^{3s}-2/2^{4s}$	(1^3)	(1^4)	4	$1+1/2^{s}-2/2^{3s}$
				(1^3)	(1^4)	64	$1-1/2^{s}$

Remarks 1.5.
- It will follow from Proposition 6.4 (3) that (2) is a special case of (1), and we will prove the two results simultaneously.
- In case (2) where k is cyclic, the splitting behavior of the primes in k is determined by congruence conditions. Also, since 2 can only split as (3) or (111) in k, only $\mathcal{L}(k,1)$ occurs and the list of possible 2-Euler factors is very short: only two cases for $M_1(s)$ and three cases for $M_{2,L}(s)$.
- As a check on our results, we used PARI/GP [25] to numerically verify the above theorems (and also Theorem 9.1) for the first 10000 totally real and the first 10000 complex cubic fields. As a further check on the consistency of our results, we also observe that the values $8M_1(1)$ are equal to the constants $c_2(k)$ in Theorem 1.2 of [7].

The formulas are much longer in the S_4 case than in the S_3 case, simply because the number of splitting types is much larger. However, the present study is in fact *simpler* than the analogous study of cubic extensions having a given quadratic resolvent. In Theorem 2.2 we will describe S_4-extensions in terms of a quadratic extension of the cubic resolvent, and since $-1\in\mathbb{Q}$ we may use Kummer theory to study this extension without first adjoining a root of unity.

In Theorem 9.1 we prove a version of our results including a signature condition. In particular, if k is totally real, we may introduce a condition into the definition of $\Phi_k(s)$ whereby we only count totally real quartic fields. It turns out that the modification to Theorem 1.4 is quite simple: one multiplies the formulas by $\frac{1}{4}$, and *removes* the signature conditions from the definitions of $\mathcal{L}_2(k)$ and $\mathcal{L}(k,1)$.

This striking phenomenon, among others (e.g., (4.3)) is vaguely reminiscent of Scholz's reflection principle [27], and especially of a version conjectured by Ohno [24] and proved by Nakagawa [23], as a consequence of a functional equation associated to the Shintani zeta function associated to the space of binary cubic forms. In work with Rubinstein-Salzedo [15], motivated by our work in [14], we used class field theory and Kummer

theory to obtain another proof of this version of Scholz reflection, together with a generalization to D_ℓ- and F_ℓ-extensions for any odd prime ℓ.

Ohno and Nakagawa's work naturally extends to the quartic setting, and in an unpublished preprint they give a conjectural generalization of their functional equation to the space of pairs of ternary quadratic forms. (This space was proved by Wright-Yukie [31] over $\mathbb{Q}$, and by Bhargava [4] over $\mathbb{Z}$, to parameterize quartic fields.) Further, Nakagawa proved a special case of their conjecture, similar to the identities implied by considering the $n = 1$ terms in Theorems 1.4 and 9.1, and he carried out additional computations with an eye towards a proof of the full conjecture. We hope, perhaps rashly, that our ideas might be useful in a proof of this conjecture.

Outline of the paper. We begin in Section 2 by recalling a parametrization of quartic fields K in term of pairs (k, K_6), where k is the cubic resolvent of K and K_6 is a quadratic extension of 'trivial norm'. This allows us to count quartic fields by counting such quadratic extensions.

Section 3 consists essentially of work of the first author, Diaz y Diaz, and Olivier [12], which establishes a version of Theorem 1.4 in an abstract setting. As this work was not published, we provide full proofs here. In Section 4 we study certain groups $C_{\mathfrak{c}^2}$ appearing in Section 3, and prove that they are essentially class groups.

In Section 5 we state a theorem establishing the possible splitting types of primes p in quartic fields and their associated pairs (k, K_6). As the proof requires lots of checking of special cases, and overlaps with some existing literature, we only sketch the proof here, but a note with complete proofs is available from the second author's website.

In Sections 6 and 7 we further study the arithmetic of quartic fields associated to characters of $C_{\mathfrak{c}^2}$; some of these results are potentially of independent interest. This then brings us to the proofs of our main results in Section 8. In Section 9 we prove a version of our main theorem counting quartic fields with prescribed signature conditions; the statement and proof of this generalization turn out to be surprisingly simple. We conclude in Section 10 with numerical examples which were helpful in double-checking our results.

2 The parametrization of quartic fields

Definition 2.1.

(1) We will say that an element $\alpha \in k^*$ (resp., an ideal $\mathfrak{a}$ of k) has square norm if $\mathcal{N}(\alpha)$ (resp., $\mathcal{N}(\mathfrak{a})$) is a square in $\mathbb{Q}^*$.[3]

(2) We will say that a quadratic extension K_6/k has *trivial norm* if there exists $\alpha \in k^* \setminus k^{*2}$ of square norm such that $K_6 = k(\sqrt{\alpha})$. (Observe for k cubic that this implies $\alpha \notin \mathbb{Q}$).

Note that if the principal ideal (α) has square norm then α has either square norm or minus square norm, but since we will only be considering such elements in *cubic* fields, this means that $\pm\alpha$ has square norm for a suitable sign.

It is fundamental to our efforts that quartic fields K with cubic resolvent k correspond to quadratic extensions K_6/k of trivial norm. We review this correspondence here.

[3] Note that in [7] there is a misprint in the definition of square norm, where "$\mathcal{N}_{K_6/k}(\alpha)$ square in k" should be replaced by what we have written, i.e., simply "α of square norm", in other words $\mathcal{N}(\alpha)$ square in $\mathbb{Q}^*$.

Theorem 2.2. *There is a correspondence between isomorphism classes of A_4 or S_4-quartic fields K, and pairs (k, K_6), where k is the cubic resolvent field of K, and K_6/k is a quadratic extension of trivial norm. Under this correspondence we have $Disc(K) = Disc(k)\mathcal{N}(\mathfrak{d}(K_6/k))$.*

If K is an S_4-field then this correspondence is a bijection, and K_6 is the unique quadratic subextension of K/k of trivial norm. If K is an A_4-field, then k has three quadratic extensions, given by adjoining a root of α or either of its nontrivial conjugates, and this correspondence is 1-to-3, with any of these fields yielding the same K (up to isomorphism).

When we apply this theorem to quartic fields $L \in \mathcal{L}_2(k)$ we still denote the corresponding sextic field by K_6.

Remark. Theorem 2.2 has rough parallels in the theory of prehomogeneous vector spaces, for example in Bhargava's work on 'higher composition laws' [3,4]. Roughly speaking, Bhargava proves that the sets (R, I), where R is a cubic ring and I is an ideal of R whose square is principal, and (Q, R), where Q is a quartic ring and R is a cubic resolvent ring of Q, are parameterized by group actions on lattices which are $\mathbb{Z}$-dual to one another.

The analogy is not exact, but as class field theory connects quadratic extensions K_6/k to index two subgroups of $\mathrm{Cl}(k)$, we can see a parallel to Bhargava's and related work.

Proof. This is well known and largely proved in Heilbronn [19] and Baily [2], but for the sake of completeness we sketch a proof.

For an A_4-quartic field K, $\widetilde{K}$ contains a unique 2-Sylow subgroup, and therefore $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ contains a unique cubic subfield k, which must be cyclic. $\widetilde{K}$ also contains three sextic fields; writing $K_6 = k(\sqrt{\alpha})$ for one of them, the other two are $k(\sqrt{\alpha'})$ for the two conjugates α' of α, so $\widetilde{K}$ contains $\mathbb{Q}(\sqrt{\mathcal{N}(\alpha)})$. However, since A_4 has no subgroup of order 6 this cannot be a quadratic extension, so α must have square norm.

Conversely, given k and $K_6 = k(\sqrt{\alpha})$, one obtains $\widetilde{K}$ by adjoining square roots of the conjugates of α, and checks that $\widetilde{K}$ is Galois over $\mathbb{Q}$ with Galois group A_4. There are four isomorphic quartic subextensions K, corresponding to the 3-Sylow subgroups of A_4. This proves the correspondence for A_4-extensions, and any of the quadratic extensions of k produce the same quartic field K (up to isomorphism).

For an S_4-quartic field K, $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ contains three conjugate 2-Sylow subgroups, corresponding to three conjugate noncyclic cubic fields k, with Galois closure $k(\sqrt{D})$ (where $D := \mathrm{Disc}(k)$), $\mathrm{Gal}(\widetilde{K}/k(\sqrt{D})) \simeq V_4 = C_2 \times C_2$, and $\mathrm{Gal}(\widetilde{K}/k) \simeq D_4$. Since D_4 contains three subgroups of size 4, there exist three quadratic subextensions of $\widetilde{K}/k$, and since S_4 has a unique subgroup of order 12, corresponding to $\mathbb{Q}(\sqrt{D})$, and $\sqrt{D} \notin k$, these subextensions are $k(\sqrt{D})$, $k(\sqrt{\alpha})$, and $k(\sqrt{\alpha D})$ for some $\alpha \in k^*$.

Now if we denote by α' and α'' the nontrivial conjugates of α and by k', k'' the corresponding conjugate fields of k, the fields $k'(\sqrt{\alpha'})$ and $k''(\sqrt{\alpha''})$ are in $\widetilde{K}$, hence $\mathbb{Q}(\sqrt{\mathcal{N}(\alpha)})$ is also. As above, since S_4 has a unique subgroup of order 12, either this is equal to $\mathbb{Q}$, in which case α has square norm, or it is equal to $\mathbb{Q}(\sqrt{D})$, in which case $\mathcal{N}(\alpha) = Da^2$ hence $\mathcal{N}(\alpha D) = D^4 a^2$, so αD has square norm.

Conversely, given a noncyclic k and $K_6 = k(\sqrt{\alpha})$ with α of square norm, one also adjoins $\sqrt{D}$, $\sqrt{\alpha D}$, and $\sqrt{\alpha'}$ for a conjugate α' of α, and checks that the resulting field contains a square root of the remaining conjugate of α and is Galois over $\mathbb{Q}$ with Galois group S_4. In particular, the proof of the next proposition describes a set of four elements of K which are permuted by this Galois group. □

Since K_6/k has trivial norm, there exists a positive integer f such that $\mathcal{N}(\mathfrak{d}(K_6/k)) = f^2$, and we will write $f = f(K)$. Thus, if we denote by $\mathcal{F}(k)$ the set of isomorphism classes of quartic extensions whose cubic resolvent is isomorphic to k we have

$$\sum_{K\in\mathcal{F}(k)} \frac{1}{|\mathrm{Disc}(K)|^s} = \frac{1}{|\mathrm{Disc}(k)|^s} \sum_{K\in\mathcal{F}(k)} \frac{1}{f(K)^{2s}} .$$

The following proposition makes the correspondence of Theorem 2.2 computationally explicit, which helped us to check numerically the correctness of our formulas.

Proposition 2.3.

1. *A defining polynomial for the cubic resolvent field of the quartic field defined by the polynomial* $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ *is given by*

$$x^3 - a_2x^2 + (a_1a_3 - 4a_0)x + 4a_0a_2 - a_1^2 - a_0a_3^2 ,$$

   whose (polynomial) discriminant is the same as the (polynomial) discriminant of the quartic.
2. *If* $K_6 = k(\sqrt{\alpha})$ *where* $\alpha \in k^* \setminus k^{*2}$ *is of square norm with characteristic polynomial* $x^3 + a_2x^2 + a_1x + a_0$, *a defining polynomial for the corresponding quartic field is given by*

$$x^4 + 2a_2x^2 - 8\sqrt{-a_0}x + a_2^2 - 4a_1 ,$$

   whose (polynomial) discriminant is 2^{12} *times the (polynomial) discriminant of the cubic.*

Proof. (1). This is well-known: if (α_i) are the four roots of the quartic, the cubic is the characteristic polynomial of $\alpha_1\alpha_2 + \alpha_3\alpha_4$.

(2). Assume that we are in the S_4 case, the A_4 case being simpler. If we denote as usual by α' and α'' the conjugates of α, then $\theta = \sqrt{\alpha}$, $\theta' = \sqrt{\alpha'}$, and $\theta'' = \sqrt{\alpha''}$ belong to $\widetilde{K}$, and we choose the square roots so that $\theta\theta'\theta'' = \sqrt{\mathcal{N}(\alpha)} = \sqrt{-a_0}$. If we set $\eta = \theta + \theta' + \theta''$, by Galois theory it is clear that η belongs to a quartic field, and more precisely the four conjugates of η are $\varepsilon\theta + \varepsilon'\theta' + \varepsilon''\theta''$ with the $\varepsilon = \pm 1$ such that $\varepsilon\varepsilon'\varepsilon'' = 1$, and a small computation shows that the characteristic polynomial of η is the one given in the proposition. This polynomial must be irreducible, because η is fixed by a subgroup of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ isomorphic to S_3, but not by all of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_4$, and there are no intermediate subgroups of S_4 of order 12. □

3 The main theorem of [7]

3.1 Statement of the main theorem

To prove our main result (Theorem 1.4), we begin by stating and proving a similar result involving sums over characters of certain ray class groups instead of over quartic fields. This result has been stated without proof in [7] and proved in the unpublished preprint [12], so we give a complete proof here.

Definition 3.1. For each ideal $\mathfrak{c} \mid 2\mathbb{Z}_k$ we define the following quantities:

1. We define a finite group $C_{\mathfrak{c}^2}$ by[4]
$$C_{\mathfrak{c}^2} = \frac{\{\mathfrak{a} \ : \ (\mathfrak{a}, \mathfrak{c}) = 1, \ \mathcal{N}(\mathfrak{a})\text{square}\}}{\left\{\mathfrak{q}^2\beta \ : \ (\mathfrak{q}^2\beta, \mathfrak{c}) = 1, \ \beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}, \ \mathcal{N}(\beta)\text{square}\right\}},$$
and we define $X_{\mathfrak{c}^2}$ to be the group of characters $\chi \in C_{\mathfrak{c}^2}$, extended to all ideals of square norm by setting $\chi(\mathfrak{a}) = 0$ if $\mathfrak{a}$ is not coprime to $\mathfrak{c}$.
2. We define $z_k(\mathfrak{c})$ to be equal to 1 or 2, with $z_k(\mathfrak{c}) = 2$ if and only if we are in one of the following cases.
   - We have $\mathfrak{c} = 2\mathbb{Z}_k$.
   - The prime 2 splits as $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$ and $\mathfrak{c} = \mathfrak{p}_1\mathfrak{p}_2$.
   - The prime 2 splits as $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$, $\mathfrak{c} = \mathfrak{p}_2$, and $\mathrm{Disc}(k) \equiv 4 \pmod 8$.
   - The prime 2 splits as $2\mathbb{Z}_k = \mathfrak{p}_1^3$ and $\mathfrak{c} = \mathfrak{p}_1^2$.

Since trivially $C_{\mathfrak{c}^2}$ has exponent dividing 2, all the elements of $X_{\mathfrak{c}^2}$ are quadratic characters, which can be applied only on ideals of square norm. With this definition, the main result of [7] is the following:

Theorem 3.2. [7,12]
$$\Phi_k(s) = \frac{2^{2-r_2(k)}}{a(k)2^{3s}} \sum_{\mathfrak{c} \mid 2\mathbb{Z}_k} \mathcal{N}\mathfrak{c}^{s-1} z_k(\mathfrak{c}) \prod_{\mathfrak{p} \mid \mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^s}\right) \sum_{\chi \in X_{\mathfrak{c}^2}} F_k(\chi, s) \ ,$$
where $r_2(k)$ is half the number of complex places of k,
$$F_k(\chi, s) = \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2} \left(1 + \frac{\chi(\mathfrak{p}_2)}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2)}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2) + \chi(\mathfrak{p}_1\mathfrak{p}_3) + \chi(\mathfrak{p}_2\mathfrak{p}_3)}{p^s}\right), \tag{3.1}$$
where in the product over $p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ it is understood that $\mathfrak{p}_1$ has degree 1 and $\mathfrak{p}_2$ has degree 2.

Remark. In [12] this is proved for relative quartic extensions of any number field. Proving Theorem 1.4 in this generality may be possible, but this would involve additional technical complications. Here we prove Theorem 3.2 only for quartic extensions of $\mathbb{Q}$, allowing some simplifications of the arguments in [12].

Our first goal is the proof of this theorem, which may be summarized as follows. By Theorem 2.2, it is enough to count quadratic extensions K_6/k of trivial norm. Our first few

[4] Note that there is a misprint in Definition 2.2 of [7], the condition $\beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}$ having been omitted from the denominator.

results parameterize such quadratic extensions and allow us to compute their discriminants, and these together with some elementary computations lead us to the preliminary result of Corollary 3.12. To proceed further we use local class field theory to study a certain quantity $|S^S_{\mathfrak{c}^2}(k)|/|C_{\mathfrak{c}^2}|$ appearing in the corollary, allowing us to obtain the more explicit formula above.

Later we will further refine this theorem and show that the groups $C_{\mathfrak{c}^2}$ are isomorphic to certain ray class groups. This will allow us to regard characters of $C_{\mathfrak{c}^2}$ as characters of Galois groups of quadratic extensions of k, allowing us to express the Euler products above in terms of splitting of prime ideals in certain quartic fields.

3.2 Proof of Theorem 3.2: Hecke, Galois, and Kummer theory

Remark. Much of this section has been taken nearly verbatim from the unpublished preprint [12], and we thank the second and third authors of that preprint for permission to include their results here.

We begin by recalling the following (easy) special case of a theorem of Hecke on Kummer extensions (see for example Theorem 10.2.9 of [6]).

Proposition 3.3. *Let k be a number field and $K_6 = k(\sqrt{\alpha})$ be a quadratic extension of k. Write $\alpha\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$ where $\mathfrak{a}$ is an integral squarefree ideal of k, and assume α is chosen so that $\mathfrak{q}$ is coprime to 2 (which can easily be done without changing the field K_6 by replacing $\mathfrak{q}$ by $\gamma\mathfrak{q}$ for a suitable element $\gamma \in k^*$).*

Then the relative ideal discriminant of K_6/k is given by the formula $\mathfrak{d}(K_6/k) = 4\mathfrak{a}/\mathfrak{c}^2$, where $\mathfrak{c}$ is the largest integral ideal of k (for divisibility) dividing $2\mathbb{Z}_k$, coprime to $\mathfrak{a}$, and such that the congruence $x^2 \equiv \alpha \pmod{{}^*\mathfrak{c}^2}$ has a solution in k, where the * has the usual multiplicative meaning of class field theory.

Definition 3.4. Let k be a number field.

(1) We say that an element $\alpha \in k^*$ is a 2-virtual unit if $\alpha\mathbb{Z}_k = \mathfrak{q}^2$ for some ideal $\mathfrak{q}$ of k, or equivalently, if $\nu_{\mathfrak{p}}(\alpha) \equiv 0 \pmod 2$ for all prime ideals $\mathfrak{p}$, and we denote by $V(k)$ the group of virtual units.

(2) We define $V^S(k)$ as the subgroup of elements of $V(k)$ having square (or equivalently, positive) norm.

(3) We define $V^+(k)$ as the subgroup of totally positive virtual units, so that $V^+(k) \subset V^S(k)$.

(4) We define the 2-Selmer group $S(k)$ of k as $S(k) = V(k)/k^{*2}$, and similarly $S^S(k) = V^S(k)/k^{*2} \subset S(k)$, and $S^+(k) = V^+(k)/k^{*2} \subset S^S(k)$.

Remarks 3.5.

- We should more properly speaking write $V_2(k)$, $S_2(k)$, etc..., but in this paper we only consider 2-virtual units.
- If k is a cubic field (or more generally a field of odd degree), which will be the case in this paper, and $\alpha \in V(k)$, then either α or $-\alpha$ belongs to $V^S(k)$.
- If k is a complex cubic field, we have $V^+(k) = V^S(k)$ and $S^+(k) = S^S(k)$, since here totally positive means positive for the unique real embedding.

Lemma 3.6. *The relative discriminant $\mathfrak{d}(K_6/k)$ of a quadratic extension K_6/k divides $4\mathbb{Z}_k$ if and only if $K_6 = k(\sqrt{\alpha})$ for some $\alpha \in V(k)$. If this is the case then $\mathfrak{d}(K_6/k)$ is a square, and K_6/k is unramified at infinity if and only if $\alpha \in V^+(k)$.*

Proof. If $\alpha \in V(k)$ then $\alpha\mathbb{Z}_k = \mathfrak{q}^2$, where as before we may choose $\mathfrak{q}$ coprime to 2, so that $\mathfrak{d}(K_6/k) = 4/\mathfrak{c}^2$ by Hecke. Conversely, let $K_6 = k(\sqrt{\alpha})$, and write $\alpha\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$, again with $\mathfrak{q}$ coprime to 2. Then $\mathfrak{d}(K_6/k) = 4\mathfrak{a}/\mathfrak{c}^2$ by Hecke, with $\mathfrak{c}$ coprime to $\mathfrak{a}$, so that $\mathfrak{d}(K_6/k) \mid 4\mathbb{Z}_k$ if and only if $\mathfrak{a} = \mathbb{Z}_k$, i.e., $\alpha \in V(k)$. For the last statement, note that K_6/k is unramified at infinity if and only if α is totally positive. □

Note that by definition, if $L \in \mathcal{L}_2(k)$ then L is totally real if k is so, hence if $K_6 = k(\sqrt{\alpha})$ we have $\alpha \in V^+(k)$.

The classification of quadratic extensions of trivial norm (see Definition 2.1) is easily done as follows.

Proposition 3.7. *There is a one-to-one correspondence between on the one hand quadratic extensions of k of trivial norm, together with the trivial extension k/k, and on the other hand pairs $(\mathfrak{a}, \overline{u})$, where $\mathfrak{a}$ is an integral, squarefree ideal of k of square norm whose class modulo principal ideals is a square in the class group of k, and $\overline{u} \in S^S(k)$.*

Proof. The exact sequence

$$1 \longrightarrow S(k) \longrightarrow \frac{k^*}{k^{*2}} \longrightarrow \frac{I(k)}{I(k)^2} \longrightarrow \frac{\mathrm{Cl}(k)}{\mathrm{Cl}(k)^2} \longrightarrow 1\ ,$$

where as usual $I(k)$ is the group of nonzero fractional ideals of k, shows the trivial fact that there is a one-to-one correspondence between quadratic extensions (including k/k) and pairs $(\mathfrak{a}, \overline{u})$ with $\mathfrak{a}$ integral and squarefree whose class belongs to $\mathrm{Cl}^2(k)$ and $\overline{u} \in S(k)$, and the trivial norm condition is equivalent to the restrictions on $(\mathfrak{a}, \overline{u})$.

We can make the correspondence explicit as follows. For each ideal $\mathfrak{a}$ as above, choose arbitrarily an ideal $\mathfrak{q}_0 = \mathfrak{q}_0(\mathfrak{a})$ and an element $\alpha_0 = \alpha_0(\mathfrak{a})$ such that $\mathfrak{a}\mathfrak{q}_0^2 = \alpha_0\mathbb{Z}_k$. Since k is a cubic field, by changing α_0 into $-\alpha_0$ if necessary we may assume that α_0 has square norm. Thus if $K_6 = k(\sqrt{\alpha})$ with α of square norm and $\alpha\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$, with $\mathfrak{a}$ integral and squarefree, then $\alpha/\alpha_0(\mathfrak{a}) \in V^S(k)$ and the corresponding pair is $(\mathfrak{a}, \overline{\alpha/\alpha_0(\mathfrak{a})})$. Conversely, for any pair $(\mathfrak{a}, \overline{u})$ as above we take $K_6 = k(\sqrt{\alpha_0(\mathfrak{a})u})$ for any lift u of $\overline{u}$. □

We now begin the computation of $\Phi_k(s)$. Recall by Theorem 2.2 that to any A_4 or S_4-quartic field there correspond $a(k)$ extensions K_6/k of trivial norm, where $a(k) = 3$ in the A_4 case and $a(k) = 1$ in the S_4 case, so by definition

$$\Phi_k(2s) = \frac{1}{a(k)} + \sum_{K \in \mathcal{F}(k)} \frac{1}{f(K)^{2s}} = \frac{1}{a(k)} \sum_{K_6/k \text{ of trivial norm}} \frac{1}{\mathcal{N}(\mathfrak{d}(K_6/k))^s}\ ,$$

where it is understood that we include the trivial extension k/k. Thus, if $(\mathfrak{a}, \overline{u})$ is as in Proposition 3.7 and $K_6 = k(\sqrt{\alpha_0(\mathfrak{a})u})$ is the corresponding quadratic extension, we know from Proposition 3.3 that $\mathfrak{d}(K_6/k) = 4\mathfrak{a}/\mathfrak{c}^2$ for an ideal $\mathfrak{c} = \mathfrak{c}(\mathfrak{a}, \overline{u})$ described in the proposition. For ease of notation, we let $\mathcal{A}$ be the set of all ideals $\mathfrak{a}$ as in Proposition 3.7 above, in other words, integral, squarefree ideals of k of square norm whose class in $\mathrm{Cl}(k)$ belongs to $\mathrm{Cl}(k)^2$.

We thus have

$$a(k)\Phi_k(2s) = \sum_{\mathfrak{a}\in\mathcal{A}} \sum_{\overline{u}\in S^S(k)} \frac{1}{\mathcal{N}(\mathfrak{d}(k(\sqrt{\alpha_0(\mathfrak{a})u})/k))^s} = \frac{1}{4^{3s}} \sum_{\mathfrak{a}\in\mathcal{A}} \frac{1}{\mathcal{N}\mathfrak{a}^s} \sum_{\overline{u}\in S^S(k)} \mathcal{N}(\mathfrak{c}(\mathfrak{a},\overline{u}))^{2s} ,$$

in other words

$$a(k)\Phi_k(s) = \frac{1}{2^{3s}} \sum_{\mathfrak{a}\in\mathcal{A}} \frac{1}{\mathcal{N}\mathfrak{a}^{s/2}} S(\mathfrak{a};s) \quad \text{with} \quad S(\mathfrak{a};s) = \sum_{\overline{u}\in S^S(k)} \mathcal{N}(\mathfrak{c}(\mathfrak{a},\overline{u}))^s = \sum_{\substack{\mathfrak{c}\mid 2\mathbb{Z}_k \\ (\mathfrak{c},\mathfrak{a})=1}} \mathcal{N}\mathfrak{c}^s T(\mathfrak{a},\mathfrak{c}),$$

where $T(\mathfrak{a},\mathfrak{c}) = \left|\left\{\overline{u}\in S^S(k) \ : \ \mathfrak{c}(\mathfrak{a},\overline{u}) = \mathfrak{c}\right\}\right|$.

Definition 3.8. We set

$$f(\mathfrak{a},\mathfrak{c}) = \left|\left\{\overline{u}\in S^S(k) : x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2} \quad \text{soluble}\right\}\right| .$$

Lemma 3.9. *We have the preliminary formula*

$$a(k)\Phi_k(s) = \frac{1}{2^{3s}} \sum_{\mathfrak{c}\mid 2\mathbb{Z}_k} \mathcal{N}\mathfrak{c}^s \prod_{\mathfrak{p}\mid\mathfrak{c}} \left(1-\mathcal{N}\mathfrak{p}^{-s}\right) \sum_{\substack{\mathfrak{a}\in\mathcal{A} \\ (\mathfrak{c},\mathfrak{a})=1}} \frac{1}{\mathcal{N}\mathfrak{a}^{s/2}} f(\mathfrak{a},\mathfrak{c}) .$$

Proof. By definition of $\mathfrak{c}(\mathfrak{a},\overline{u})$, for every $\mathfrak{c} \mid 2\mathbb{Z}_k$ we have

$$f(\mathfrak{a},\mathfrak{c}) = \sum_{\substack{\mathfrak{c}\mid\mathfrak{c}_1\mid 2\mathbb{Z}_k \\ (\mathfrak{c}_1,\mathfrak{a})=1}} T(\mathfrak{a},\mathfrak{c}_1) .$$

By dual Möbius inversion we obtain

$$T(\mathfrak{a},\mathfrak{c}) = \sum_{\substack{\mathfrak{c}\mid\mathfrak{c}_1\mid 2\mathbb{Z}_k \\ (\mathfrak{c}_1,\mathfrak{a})=1}} \mu_k\left(\frac{\mathfrak{c}_1}{\mathfrak{c}}\right) f(\mathfrak{a},\mathfrak{c}_1) ,$$

where μ_k is the Möbius function on ideals of k. Replacing in the formula for $S(\mathfrak{a};s)$, we thus have

$$\begin{aligned} S(\mathfrak{a};s) &= \sum_{\substack{\mathfrak{c}\mid 2\mathbb{Z}_k \\ (\mathfrak{c},\mathfrak{a})=1}} \mathcal{N}\mathfrak{c}^s T(\mathfrak{a},\mathfrak{c}) = \sum_{\substack{\mathfrak{c}_1\mid 2\mathbb{Z}_k \\ (\mathfrak{c}_1,\mathfrak{a})=1}} f(\mathfrak{a},\mathfrak{c}_1) \sum_{\mathfrak{c}\mid\mathfrak{c}_1} \mu_k(\mathfrak{c}_1/\mathfrak{c})\mathcal{N}\mathfrak{c}^s \\ &= \sum_{\substack{\mathfrak{c}_1\mid 2\mathbb{Z}_k \\ (\mathfrak{c}_1,\mathfrak{a})=1}} f(\mathfrak{a},\mathfrak{c}_1)\mathcal{N}\mathfrak{c}_1^s \prod_{\mathfrak{p}\mid\mathfrak{c}_1} \left(1-\mathcal{N}\mathfrak{p}^{-s}\right) . \end{aligned}$$

Replacing in the formula for $\Phi_k(s)$ and writing $\mathfrak{c}$ for $\mathfrak{c}_1$, we obtain (when $(\mathfrak{c},\mathfrak{a}) = 1$)

$$\begin{aligned} a(k)\Phi_k(s) &= \frac{1}{2^{3s}} \sum_{\mathfrak{a}\in\mathcal{A}} \frac{1}{\mathcal{N}\mathfrak{a}^{s/2}} \sum_{\substack{\mathfrak{c}\mid 2\mathbb{Z}_k \\ (\mathfrak{c},\mathfrak{a})=1}} f(\mathfrak{a},\mathfrak{c})\mathcal{N}\mathfrak{c}^s \prod_{\mathfrak{p}\mid\mathfrak{c}} \left(1-\mathcal{N}\mathfrak{p}^{-s}\right) \\ &= \frac{1}{2^{3s}} \sum_{\mathfrak{c}\mid 2\mathbb{Z}_k} \mathcal{N}\mathfrak{c}^s \prod_{\mathfrak{p}\mid\mathfrak{c}} \left(1-\mathcal{N}\mathfrak{p}^{-s}\right) \sum_{\substack{\mathfrak{a}\in\mathcal{A} \\ (\mathfrak{c},\mathfrak{a})=1}} \frac{1}{\mathcal{N}\mathfrak{a}^{s/2}} f(\mathfrak{a},\mathfrak{c}) , \end{aligned}$$

proving the lemma. □

To compute $f(\mathfrak{a},\mathfrak{c})$ we introduce the following definitions.

Definition 3.10. Let k be a cubic field and let $\mathfrak{c}$ be an ideal of k dividing $2\mathbb{Z}_k$.

(1) We define the square ray class group modulo $\mathfrak{c}^2$ by

$$\mathrm{Cl}^S_{\mathfrak{c}^2}(k) = \frac{\{\mathfrak{a} \ : \ (\mathfrak{a},\mathfrak{c}) = 1,\ \mathcal{N}(\mathfrak{a}) \quad \text{square}\}}{\{\beta\mathbb{Z}_k \ : \ \beta \equiv 1 \pmod{{}^*\mathfrak{c}^2},\ \mathcal{N}(\beta) \quad \text{square}\}} .$$

(2) We define the following subgroup of $\mathrm{Cl}^S_{\mathfrak{c}^2}(k)$:

$$D_{\mathfrak{c}^2} = \frac{\left\{\mathfrak{q}^2\beta \ : \ (\mathfrak{q}^2\beta,\mathfrak{c}) = 1,\ \beta \equiv 1 \pmod{{}^*\mathfrak{c}^2},\ \mathcal{N}(\beta) \quad \text{square}\right\}}{\left\{\beta\mathbb{Z}_k \ : \ \beta \equiv 1 \pmod{{}^*\mathfrak{c}^2},\ \mathcal{N}(\beta) \quad \text{square}\right\}} .$$

Note that the group $C_{\mathfrak{c}^2}$, defined in Definition 3.1, is canonically isomorphic to $\mathrm{Cl}^S_{\mathfrak{c}^2}(k)/D_{\mathfrak{c}^2}$.

(3) We define the ordinary ray Selmer group modulo $\mathfrak{c}^2$ by

$$S_{\mathfrak{c}^2}(k) = \{\overline{u} \in S(k) \ : \ x^2 \equiv u \pmod{{}^*\mathfrak{c}^2} \quad \text{soluble}\}.$$

(4) We define the square Selmer group modulo $\mathfrak{c}^2$ by

$$S^S_{\mathfrak{c}^2}(k) = \{\overline{u} \in S_{\mathfrak{c}^2}(k) \ : \ \mathcal{N}(u) \quad \text{square}\} .$$

(Observe that our Selmer group definitions do not depend on the choice of lifts $\overline{u}$.)

(5) Set $Z_{\mathfrak{c}} = (\mathbb{Z}_k/\mathfrak{c}^2)^*$, and let $Z^S_{\mathfrak{c}}$ be the subgroup of elements of $Z_{\mathfrak{c}}$ which have a lift to $\mathbb{Z}_k$ whose norm is a square. We define $z_k(\mathfrak{c})$ as the index of $Z^S_{\mathfrak{c}}$ in $Z_{\mathfrak{c}}$. (In Proposition 3.20 we will prove that this intrinsic definition of $z_k(\mathfrak{c})$ agrees with Definition 3.1.)

Remark. Note that if $u \in V(k)$ then $\pm\mathcal{N}(u)$ is a square for a suitable sign, so in the definition above the condition $\mathcal{N}(u)$ square can be replaced by $\mathcal{N}(u) > 0$. (This simplification did not apply in [12], as the base field there was not necessarily $\mathbb{Q}$).

The value of $f(\mathfrak{a},\mathfrak{c})$ is then given by the following proposition.

Proposition 3.11. *Let $\mathfrak{a} \in \mathcal{A}$ with $(\mathfrak{a},\mathfrak{c}) = 1$ be as above. We have $f(\mathfrak{a},\mathfrak{c}) \neq 0$ if and only if the class of $\mathfrak{a}$ in $Cl^S_{\mathfrak{c}^2}(k)$ belongs in fact to $D_{\mathfrak{c}^2}$, in which case $f(\mathfrak{a},\mathfrak{c}) = |S^S_{\mathfrak{c}^2}(k)|$.*

Proof. This is just a matter of rewriting the definitions. Assume that there exists $\overline{u} \in S^S(k)$ such that $x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}$ has a solution. This means that we can write $\beta x^2 = \alpha_0 u$ for some $\beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}$. Since $u \in V(k)$ we can write $u\mathbb{Z}_k = \mathfrak{q}_1^2$ for some ideal $\mathfrak{q}_1$. Thus

$$\mathfrak{a} = \alpha_0\mathfrak{q}_0^{-2} = (\beta x^2/u)\mathfrak{q}_0^{-2} = \beta(x/(\mathfrak{q}_0\mathfrak{q}_1))^2 .$$

In addition, since u and α_0 are of square norm in K, β is also of square norm, and since $\mathfrak{a}$ is coprime to $\mathfrak{c}$, the class of $\mathfrak{a}$ in $\mathrm{Cl}^S_{\mathfrak{c}^2}(k)$ belongs to $D_{\mathfrak{c}^2}$. The proof of the converse retraces the above steps and is left to the reader, proving the first part of the proposition. For the second part, assume that there exists $\overline{v} \in S^S(k)$ and $y \in k^*$ such that $y^2 \equiv \alpha_0 v \pmod{{}^*\mathfrak{c}^2}$. Then the solubility of $x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}$ is equivalent to that of $(x/y)^2 \equiv (u/v) \pmod{{}^*\mathfrak{c}^2}$, in other words to $\overline{u} \in \overline{v}\, S^S_{\mathfrak{c}^2}(k)$ whose cardinality is equal to that of $S^S_{\mathfrak{c}^2}(k)$, proving the proposition. □

Corollary 3.12. *We have*

$$a(k)\Phi_k(s) = \frac{1}{2^{3s}} \sum_{\mathfrak{c} \mid 2\mathbb{Z}_k} \frac{\left|S^S_{\mathfrak{c}^2}(k)\right|}{|C_{\mathfrak{c}^2}|} \mathcal{N}\mathfrak{c}^s \prod_{\mathfrak{p} \mid \mathfrak{c}} \left(1 - \mathcal{N}\mathfrak{p}^{-s}\right) \sum_{\chi \in X_{\mathfrak{c}^2}} F_k(\chi, s)\,, \quad \textit{with}$$

$$F_k(\chi,s) = \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2} \left(1 + \frac{\chi(\mathfrak{p}_2)}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2)}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2) + \chi(\mathfrak{p}_1\mathfrak{p}_3) + \chi(\mathfrak{p}_2\mathfrak{p}_3)}{p^s}\right).$$

Proof. By the above proposition we have

$$a(k)\Phi_k(s) = \frac{1}{2^{3s}} \sum_{\mathfrak{c} \mid 2\mathbb{Z}_k} \left|S^S_{\mathfrak{c}^2}(k)\right| \mathcal{N}\mathfrak{c}^s \prod_{\mathfrak{p} \mid \mathfrak{c}} \left(1 - \mathcal{N}\mathfrak{p}^{-s}\right) \sum_{\substack{\mathfrak{a} \in \mathcal{A} \\ \overline{\mathfrak{a}} \in D_{\mathfrak{c}^2}}} \frac{1}{\mathcal{N}\mathfrak{a}^{s/2}}\,.$$

Note first that if $\overline{\mathfrak{a}} \in D_{\mathfrak{c}^2}$ then the class of $\mathfrak{a}$ in $\mathrm{Cl}(k)$ belongs to $\mathrm{Cl}(k)^2$, so we may replace $\mathfrak{a} \in \mathcal{A}$ by $\mathfrak{a} \in \mathcal{A}'$, where the condition that the class of $\mathfrak{a}$ is in $\mathrm{Cl}(k)^2$ is removed. Since $C_{\mathfrak{c}^2} = \mathrm{Cl}^S_{\mathfrak{c}^2}(k)/D_{\mathfrak{c}^2}$, we can detect the condition $\overline{\mathfrak{a}} \in D_{\mathfrak{c}^2}$ by summing over characters of $C_{\mathfrak{c}^2}$, hence

$$a(k)\Phi_k(s) = \frac{1}{2^{3s}} \sum_{\mathfrak{c} \mid 2\mathbb{Z}_k} \frac{\left|S^S_{\mathfrak{c}^2}(k)\right|}{|C_{\mathfrak{c}^2}|} \mathcal{N}\mathfrak{c}^s \prod_{\mathfrak{p} \mid \mathfrak{c}} \left(1 - \mathcal{N}\mathfrak{p}^{-s}\right) \sum_{\chi \in X_{\mathfrak{c}^2}} \sum_{\mathfrak{a} \in \mathcal{A}'} \frac{\chi(\mathfrak{a})}{\mathcal{N}\mathfrak{a}^{s/2}}\,.$$

The last sum is clearly multiplicative (because we removed the condition on $\mathrm{Cl}(k)^2$), and looking at the five possible decomposition types of primes and keeping only the integral squarefree ideals of square norm proves the corollary. □

3.3 Computation of $|S^S_{\mathfrak{c}^2}(k)|/|C_{\mathfrak{c}^2}|$

The above computations were straightforward. It remains to compute $|S^S_{\mathfrak{c}^2}(k)|/|C_{\mathfrak{c}^2}|$, and this is more difficult. In the course of this computation we will prove some intermediate results which we will further use in this paper.

Proposition 3.13. *Recall from Definition 3.10 that we have set $Z_{\mathfrak{c}} = (\mathbb{Z}_k/\mathfrak{c}^2)^*$, and that $C_{\mathfrak{c}^2} = Cl^S_{\mathfrak{c}^2}(k)/D_{\mathfrak{c}^2}$.*

(1) There exists a natural exact sequence

$$1 \longrightarrow S^S_{\mathfrak{c}^2}(k) \longrightarrow S^S(k) \longrightarrow \frac{Z^S_{\mathfrak{c}}}{Z^2_{\mathfrak{c}}} \longrightarrow C_{\mathfrak{c}^2} \longrightarrow C_{(1)} \longrightarrow 1\,. \tag{3.2}$$

(2) There exists a natural exact sequence

$$1 \longrightarrow U(k)/U(k)^2 \longrightarrow S(k) \longrightarrow Cl(k)[2] \longrightarrow 1\,, \tag{3.3}$$

and a canonical isomorphism $S^S(k) \simeq S(k)/\{\pm 1\}$.

(3) We have a canonical isomorphism $C_{(1)} \simeq Cl(k)/Cl(k)^2$.

Proof. (1). All the maps are clear, and the exactness is immediate everywhere except for the surjectivity of the final map. Let $\mathfrak{a}$ be an ideal of square norm, so that $\mathcal{N}(\mathfrak{a}) = q^2$ with $q \in \mathbb{Q}$. If we set $\mathfrak{b} = \mathfrak{a}q^{-1}$ it is clear that $\mathfrak{b}/\mathcal{N}(\mathfrak{b}) = \mathfrak{a}$. By the approximation theorem, we can find $\beta \in k$ such that $\beta\mathfrak{b}$ is integral and coprime to $2\mathbb{Z}_k$. It follows that $\mathcal{N}(\beta\mathfrak{b})$ is coprime to 2, hence $(\beta/\mathcal{N}(\beta))\mathfrak{b}/\mathcal{N}(\mathfrak{b}) = (\beta/\mathcal{N}(\beta))\mathfrak{a}$ is coprime to $2\mathbb{Z}_k$, hence to $\mathfrak{c}^2$. Since $\beta/\mathcal{N}(\beta)$ is an element of square norm, we conclude that $(\beta/\mathcal{N}(\beta))\mathfrak{a}$ is in the same class as

$\mathfrak{a}$ in $\mathrm{Cl}^S(k)$ and is coprime to $\mathfrak{c}^2$, proving the surjectivity of the natural map from $\mathrm{Cl}^S_{\mathfrak{c}^2}(k)$ to $\mathrm{Cl}^S(k)$, hence that of the last map in the sequence above.

(2) and (3). The exact sequence is equivalent to the definition of $S(k)$, and the isomorphism $S(k)/\{\pm1\}\simeq S^S(k)$ is simply the map induced by $u \mapsto \mathrm{sign}(\mathcal{N}(u))u$. Finally (3) will be proved in Proposition 4.1 below. □

Corollary 3.14. *We have*

$$\frac{|S^S_{\mathfrak{c}^2}(k)|}{|C_{\mathfrak{c}^2}|} = 2^{2-r_2(k)}\frac{z_k(\mathfrak{c})}{\mathcal{N}(\mathfrak{c})}\,,$$

where we recall from Definition 3.10 that $z_k(\mathfrak{c}) = \left[Z_{\mathfrak{c}} : Z^S_{\mathfrak{c}}\right]$.

Proof. Using the exact sequences and isomorphisms, the equality $|\mathrm{Cl}(k)[2]| = |\mathrm{Cl}(k)/\mathrm{Cl}(k)^2|$ and Dirichlet's unit theorem telling us that $|U(k)/U(k)^2| = 2^{r_1(k)+r_2(k)}$ we have

$$\begin{aligned}|S^S_{\mathfrak{c}^2}(k)||Z^S_{\mathfrak{c}}/Z_{\mathfrak{c}^2}||C_{(1)}| = |S^S(k)||C_{\mathfrak{c}^2}| = |S(k)||C_{\mathfrak{c}^2}|/2 = |U(k)/U(k)^2||\mathrm{Cl}(k)[2]\,||C_{\mathfrak{c}^2}|/2\\ = 2^{r_1(k)+r_2(k)}|\mathrm{Cl}(k)/\mathrm{Cl}(k)^2||C_{\mathfrak{c}^2}|/2 = 2^{r_1(k)+r_2(k)-1}|C_{(1)}||C_{\mathfrak{c}^2}|\,,\end{aligned}$$

in other words

$$|S^S_{\mathfrak{c}^2}(k)|/|C_{\mathfrak{c}^2}| = 2^{r_1(k)+r_2(k)-1}/|Z^S_{\mathfrak{c}}/Z^2_{\mathfrak{c}}|\,.$$

Since k is a cubic field we have $r_1(k) + r_2(k) = 3 - r_2(k)$, so the corollary is immediate from the following lemma: □

Lemma 3.15. *The map* $x \mapsto x^2$ *induces a natural isomorphism between* $(\mathbb{Z}_k/\mathfrak{c})^*$ *and* $Z^2_{\mathfrak{c}}$. *In particular,* $|Z^2_{\mathfrak{c}}| = \phi_k(\mathfrak{c})$, *where* ϕ_k *denotes the ideal Euler* ϕ *function for the field* k, $|Z_{\mathfrak{c}}/Z^2_{\mathfrak{c}}| = \mathcal{N}(\mathfrak{c})$ *and* $|Z^S_{\mathfrak{c}}/Z^2_{\mathfrak{c}}| = \mathcal{N}(\mathfrak{c})/z_k(\mathfrak{c})$.

Proof. Since $\mathfrak{c} \mid 2\mathbb{Z}_k$, it is immediately checked that the congruence $x^2 \equiv 1 \pmod{{}^*\mathfrak{c}^2}$ is equivalent to $x \equiv 1 \pmod{{}^*\mathfrak{c}}$, which proves the first result. Now it is well-known and easy to show that we have the explicit formula $\phi_k(\mathfrak{c}) = \mathcal{N}(\mathfrak{c})\prod_{\mathfrak{p}|\mathfrak{c}}(1 - 1/\mathcal{N}\mathfrak{p})$. It follows in particular that $|Z_{\mathfrak{c}}| := |\mathbb{Z}_k/\mathfrak{c}^2| = \phi_k(\mathfrak{c}^2) = \mathcal{N}(\mathfrak{c})\phi_k(\mathfrak{c})$, so that $|Z_{\mathfrak{c}}/Z^2_{\mathfrak{c}}| = \mathcal{N}(\mathfrak{c}) = |Z_{\mathfrak{c}}/Z^S_{\mathfrak{c}}||Z^S_{\mathfrak{c}}/Z^2_{\mathfrak{c}}|$, proving the lemma by definition of $z_k(\mathfrak{c})$. □

It remains to prove the formula for $z_k(\mathfrak{c})$ given in Definition 3.1.

3.4 Computation of $z_k(\mathfrak{c})$

We first prove a series of lemmas.

Lemma 3.16. *For each* $\mathfrak{c}|2\mathbb{Z}_k$ *we have* $z_k(\mathfrak{c}) = 1$ *if there exists an element* β *of square norm such that* $\beta \equiv -1 \pmod{\mathfrak{c}^2}$, *and* $z_k(\mathfrak{c}) = 2$ *otherwise.*

In particular, $z_k(2\mathbb{Z}_k) = 2$.

Proof. Let $\overline{\alpha} \in (\mathbb{Z}_k/\mathfrak{c}^2)^*$, and choose a lift of $\overline{\alpha}$ to $\mathbb{Z}_k$ which is coprime to 2, which is always possible. Then $\mathcal{N}(\alpha)$ is odd hence $\mathcal{N}(\alpha) \equiv \pm1 \pmod 4$. If $\mathcal{N}(\alpha) \equiv 1 \pmod 4$, then $\alpha/\mathcal{N}(\alpha) \equiv \alpha \pmod 4$ and a fortiori modulo $\mathfrak{c}^2$, and is of square norm.

If β as described in the lemma exists, and $\mathcal{N}(\alpha) \equiv -1 \pmod 4$, then $\alpha\beta/\mathcal{N}(\alpha) \equiv \alpha \pmod{\mathfrak{c}^2}$ and is of square norm, so that $z_k(\mathfrak{c}) = 1$. If no such β exists, then -1 lacks a lift of square norm so that $z_k(\mathfrak{c}) \geq 2$. However, for each $\overline{\alpha}$, one of $\overline{\alpha}$ or $-\overline{\alpha}$ has a lift of square norm: again choose a lift α of $\overline{\alpha}$ coprime to 2, and either $\mathcal{N}(\alpha) \equiv 1 \pmod 4$ and $\alpha/\mathcal{N}(\alpha) \equiv \alpha \pmod 4$ is of square norm, or this is true with α replaced by $-\alpha$. Therefore $z_k(\mathfrak{c}) = 2$.

For $\mathfrak{c} = (2)$, the condition $\beta \equiv -1 \pmod 4$ implies $\mathcal{N}(\beta) \equiv -1 \pmod 4$, so that $\mathcal{N}(\beta)$ cannot be a square. □

Lemma 3.17. *An element $\beta \in k$ is of square norm if and only if $\beta = \alpha/\mathcal{N}(\alpha)$ for some $\alpha \in k$.*

Proof. Given α, we see immediately that β is of square norm; conversely, given β, take $\alpha = \beta/\sqrt{\mathcal{N}(\beta)}$. □

Of course this is also equivalent to the condition that $\beta = \mathcal{N}(\alpha')/\alpha'$ for some $\alpha' \in k$.

Lemma 3.18. *If $\mathfrak{p}$ is an unramified prime ideal dividing 2 then $z_k(2/\mathfrak{p}) = 1$.*

Proof. Set $\mathfrak{c} = 2/\mathfrak{p}$. Since $\mathfrak{p}$ is unramified we have $\mathfrak{p} \nmid \mathfrak{c}$, so the inclusions $k \hookrightarrow k_\mathfrak{p}$ and $k \hookrightarrow k_\mathfrak{c}$ induce an isomorphism $k \otimes \mathbb{Q}_2 \simeq k_\mathfrak{c} \times k_\mathfrak{p}$; here $k_\mathfrak{p}$ is the completion of k at $\mathfrak{p}$ and $k_\mathfrak{c}$ is isomorphic to the product of the completions of k at primes other than $\mathfrak{p}$. Any element γ of $k \otimes \mathbb{Q}_2$ can thus be written in the form $(\gamma_\mathfrak{c}, \gamma_\mathfrak{p})$ and we have

$$\mathcal{N}(\gamma) = \mathcal{N}_{k_\mathfrak{c}/\mathbb{Q}_2}(\gamma_c)\mathcal{N}_{k_\mathfrak{p}/\mathbb{Q}_2}(\gamma_\mathfrak{p}) .$$

It follows that $\mathcal{N}(\gamma)/\gamma = (\alpha_\mathfrak{c}, \alpha_\mathfrak{p})$ with

$$\alpha_\mathfrak{c} = \frac{\mathcal{N}_{k_\mathfrak{c}/\mathbb{Q}_2}(\gamma_c)}{\gamma_c}\mathcal{N}_{k_\mathfrak{p}/\mathbb{Q}_2}(\gamma_\mathfrak{p}) .$$

We choose $\gamma_\mathfrak{c} = 1$. Furthermore, since $\mathfrak{p}$ is unramified, we know that the local norm from $k_\mathfrak{p}$ to $\mathbb{Q}_2$ is surjective on units, so in particular there exists $\gamma_\mathfrak{p} \in k_\mathfrak{p}$ such that $\mathcal{N}_{k_\mathfrak{p}/\mathbb{Q}_2}(\gamma_\mathfrak{p}) = -1$. It follows that for such a γ, we have $\mathcal{N}(\gamma)/\gamma = (-1, u)$ for some $u \in k_\mathfrak{p}$, and in particular the local component at $\mathfrak{c}$ of $\mathcal{N}(\gamma)/\gamma$ is equal to -1. By density (or, equivalently, by the approximation theorem), we can find γ in the global field k such that $\mathcal{N}(\gamma)/\gamma \equiv -1 \pmod{\mathfrak{c}^m}$ for any $m \geq 1$, and in particular for $m = 2$. If we set $\beta = \mathcal{N}(\gamma)/\gamma$, it is clear that β is of square norm and $\beta \equiv -1 \pmod{\mathfrak{c}^2}$. We conclude thanks to Lemma 3.16. □

Lemma 3.19. *Let $\alpha \in k$ be such that $\alpha/2 \in \mathbb{Z}_k$ and $\alpha/4 \in \mathfrak{D}^{-1}(k)$, where $\mathfrak{D}^{-1}(k)$ denotes the codifferent of k. Then the characteristic polynomial of α is congruent to X^3 modulo 4, and in particular the norm of $\alpha - 1$ is not a square in $\mathbb{Q}$.*

Proof. Let $X^3 - tX^2 + sX - n$ be the characteristic polynomial of α. Since $\alpha/4 \in \mathfrak{D}^{-1}(k)$, we know that $t = \mathrm{Tr}(\alpha) \equiv 0 \pmod 4$. Furthermore, since $\alpha/2 \in \mathbb{Z}_k$, we also have $\mathrm{Tr}(\alpha(\alpha/2)) \equiv 0 \pmod 4$, hence $\mathrm{Tr}(\alpha^2) \equiv 0 \pmod 8$, so $s = (\mathrm{Tr}(\alpha)^2 - \mathrm{Tr}(\alpha^2))/2 \equiv 0 \pmod 4$. Finally we have $n = \mathcal{N}(\alpha) \equiv 0 \pmod 8$, and in particular $n \equiv 0 \pmod 4$, proving the first statement (note that in fact we can easily prove that $n \equiv 0 \pmod{16}$, but we

do not need this). It follows that the characteristic polynomial of $\alpha - 1$ is congruent to $(X+1)^3$ modulo 4, hence that the norm of $\alpha - 1$ is congruent to -1 modulo 4, so cannot be a square in $\mathbb{Q}$. □

We can now finally compute $z_k(\mathfrak{c})$ in all cases:

Theorem 3.20. *The definition of $z_k(\mathfrak{c})$ in Proposition 3.10 (5) matches the explicit formula of Definition 3.1.*

Proof. We have trivially $z_k((1)) = 1$, and by Lemma 3.16 we have $z_k((2)) = 2$, so we assume that $\mathfrak{c} \neq (1)$ and $\mathfrak{c} \neq (2)$. Lemma 3.16 also implies that $z_k(\mathfrak{c}') \leq z_k(\mathfrak{c})$ for $\mathfrak{c}'|\mathfrak{c}$.

We consider the possible splitting types of 2 in k.

- Assume that 2 is unramified, and let $\mathfrak{p}$ be a prime ideal dividing $2/\mathfrak{c}$. By Lemma 3.18 we have $z_k(2/\mathfrak{p}) = 1$, and since $\mathfrak{c} \mid 2/\mathfrak{p}$ we have $z_k(\mathfrak{c}) \mid z_k(2/\mathfrak{p})$ so $z_k(\mathfrak{c}) = 1$.
- Assume that 2 is totally ramified as $2\mathbb{Z}_k = \mathfrak{p}^3$. If $\mathfrak{c} = \mathfrak{p}$ then $\beta = 1$ is of square norm and is such that $\beta \equiv -1 \pmod{\mathfrak{c}^2}$, hence $z_k(\mathfrak{p}) = 1$. If $\mathfrak{c} = \mathfrak{p}^2$, let β be any element such that $\beta \equiv -1 \pmod{\mathfrak{c}^2}$, and set $\alpha = \beta + 1 \in 2\mathfrak{p}$. Since 2 is tamely ramified, we have $\mathfrak{D}(k) = \mathfrak{p}^2\mathfrak{a}$ for some ideal $\mathfrak{a}$ coprime to 2. It follows that $\alpha/4 \in \mathfrak{p}^{-2} \subset \mathfrak{D}^{-1}(k)$, and of course $\alpha/2 \in \mathfrak{p} \subset \mathbb{Z}_k$. Applying Lemma 3.19, we deduce that $\mathcal{N}(\beta)$ cannot be a square, showing that $z_k(\mathfrak{p}^2) = 2$.
- Assume that 2 is partially ramified as $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$ and that $\mathfrak{p}_1 \mid \mathfrak{c}$. Lemma 3.18 implies that $z_k\left(\mathfrak{p}_1^2\right) = 1$, hence also $z_k(\mathfrak{p}_1) = 1$. If $\mathfrak{c} = \mathfrak{p}_1\mathfrak{p}_2$, let $\beta \equiv -1 \pmod{\mathfrak{c}^2}$, and set $\alpha = \beta + 1 \in 2\mathfrak{p}_2$. Here 2 is wildly ramified, so we also deduce that $\mathfrak{D}(k) = \mathfrak{p}_1^2\mathfrak{a}$ for some $\mathfrak{a}$ not necessarily coprime to 2. As above, we deduce that $\alpha/4 \in \mathfrak{p}_1^{-2} \subset \mathfrak{D}^{-1}(k)$ and $\alpha/2 \in \mathfrak{p}_2 \subset \mathbb{Z}_k$, so that by Lemma 3.19, $\mathcal{N}(\beta)$ cannot be a square, hence $z_k(\mathfrak{p}_1\mathfrak{p}_2) = 2$.
- Assume finally that 2 is partially ramified as $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$ and that $\mathfrak{p}_1 \nmid \mathfrak{c}$, in other words $\mathfrak{c} = \mathfrak{p}_2$. We use Lemma 3.17 and the same local reasoning as for the proof of Lemma 3.18. Setting $k_i = k_{\mathfrak{p}_i}$, we can write $k \otimes \mathbb{Q}_2 \simeq k_1 \times k_2$. If $\gamma = (\gamma_1, \gamma_2)$ then as before we have $\mathcal{N}(\gamma)/\gamma = (\alpha_1, \alpha_2)$ with $\alpha_2 = N_{k_1/\mathbb{Q}_2}(\gamma_1)$, since we can identify k_2 with $\mathbb{Q}_2$. Since 2 is a local uniformizer for the unramified prime ideal $\mathfrak{p}_2$, it follows that we have $z_k(\mathfrak{p}_2) = 1$ if and only if we can solve $\alpha_2 \equiv -1 \pmod{4}$, hence if and only if there exists a norm congruent to -1 modulo 4 in the local ramified extension $k_1/\mathbb{Q}_2$. Up to isomorphism, there are 6 possible such extensions $k_1 = \mathbb{Q}_2(\sqrt{D})$ with $D = -4, -8, -24, 8, 12$, and 24 (the extension corresponding to $D = -3$ is of course unramified). By inspection[5] , we see that -1 is a norm in the extensions corresponding to $D = -24$ and $D = 8$, and that 3 is a norm in the extensions corresponding to $D = -8$ and $D = 24$. As $D \equiv 0 \pmod 8$ if and only if $\mathrm{Disc}(k) \equiv 0 \pmod 8$, this finishes the proof of the theorem in the case $\mathrm{Disc}(k) \equiv 0 \pmod 8$.

  In case $\mathrm{Disc}(k) \equiv 4 \pmod 8$, we have $D = -4$ or $D = 12$, and since the equations $x^2 + y^2 = -1$ and $x^2 - 3y^2 = -1$ are not soluble in $\mathbb{Q}_2$ (they do not have solutions modulo 4) it follows that -1 is not a norm, so that $z_k(\mathfrak{p}_2) = 2$. □

[5] For example, $1^2 + 6 \cdot 1^2 = 7 \equiv -1 \pmod 8$, and as the conductor of $\mathbb{Q}_2(\sqrt{-6}) = \mathbb{Q}_2(\sqrt{-24})$ is 2^3, this congruence can be lifted to a solution in $\mathbb{Q}_2$.

Replacing the value of $z_k(\mathfrak{c})$ given by Definition 3.1 in the formula for $|S^S_{\mathfrak{c}^2}(k)|/|C_{\mathfrak{c}^2}|$ given in Corollary 3.14 and then in the formula for $\Phi_k(s)$ given by Corollary 3.12 finishes the proof of Theorem 3.2.

4 Study of the groups $C_{\mathfrak{c}^2}$

We denote by $\mathrm{rk}_2(k)$ the 2-rank of $\mathrm{Cl}(k)$, and by $\mathrm{rk}_2^+(k)$ the 2-rank of the narrow class group $\mathrm{Cl}^+(k)$.

Proposition 4.1. *Let $C_{(4)}$ be defined as in Definition 3.1.*

1. *The map $\phi : \mathfrak{a} \to \mathfrak{a}/\mathcal{N}(\mathfrak{a})$ induces isomorphisms*

$$Cl(k)/Cl(k)^2 \xrightarrow{\phi} C_{(1)} , \tag{4.1}$$

$$Cl_{(4)}(k)/Cl_{(4)}(k)^2 \xrightarrow{\phi} C_{(4)} , \tag{4.2}$$

   with the inverse map induced by $\phi^{-1} : \mathfrak{b} \to \mathfrak{b}/\sqrt{N(\mathfrak{b})}$.
2. *We have either $|C_{(4)}| = 2|C_{(1)}|$ or $|C_{(4)}| = |C_{(1)}|$. Moreover, $|C_{(4)}| = |C_{(1)}|$ if and only if k is totally real and $rk_2^+(k) = rk_2(k)$, i.e., if and only if k is totally real and there does not exist a nonsquare totally positive unit.*
3. *If $\mathfrak{c}'|\mathfrak{c}$ and $|C_{\mathfrak{c}^2}| = |C_{(1)}|$ then $C_{\mathfrak{c}'^2} \simeq C_{(1)}$ also; and if $\mathfrak{c}'|\mathfrak{c}$ and $|C_{\mathfrak{c}'^2}| = |C_{(4)}|$ then $C_{\mathfrak{c}^2} \simeq C_{(4)}$ also.*
   In particular, if $|C_{(1)}| = |C_{(4)}|$ then $C_{\mathfrak{c}^2} \simeq Cl(k)/Cl(k)^2 \simeq Cl_{(4)}(k)/Cl_{(4)}(k)^2$ for every $\mathfrak{c}|(2)$.

Proof. (1). It is easily checked that ϕ^{-1} and ϕ yield inverse bijections between the group of fractional ideals of k of square norm and all fractional ideals of k. Both ϕ and ϕ^{-1} map principal ideals to principal ideals, and ϕ maps any square ideal to a square ideal. Also it is clear that $\alpha \equiv 1 \pmod{4\mathbb{Z}_k}$ implies $\mathcal{N}(\alpha) \equiv 1 \pmod 4$, so the maps (4.1) and (4.2) are well-defined homomorphisms. Conversely, it is clear that the map ϕ^{-1} from $C_{(1)}$ to $\mathrm{Cl}(k)/\mathrm{Cl}(k)^2$ is also well-defined. Consider ϕ^{-1} on $C_{(4)}$: we have $\phi^{-1}(\mathfrak{q}^2\beta) = \mathfrak{q}^2\beta/\mathcal{N}(\mathfrak{q})\sqrt{\mathcal{N}(\beta)}$, and since $\beta \equiv 1 \pmod{{}^*4\mathbb{Z}_k}$, the class of $\phi^{-1}(\mathfrak{q}^2\beta)$ in $\mathrm{Cl}_{(4)}(k)/\mathrm{Cl}_{(4)}(k)^2$ is the same as that of $a\mathbb{Z}_k$ with $a = \mathcal{N}(\mathfrak{q})\sqrt{\mathcal{N}(\beta)}$. However $a \in \mathbb{Q}$, so $a \equiv \pm 1 \pmod{{}^*4}$, and $a\mathbb{Z}_k = -a\mathbb{Z}_k$, so the class of $\phi^{-1}(\mathfrak{q}^2\beta)$ is trivial, proving that ϕ^{-1} is a well-defined map from $C_{(4)}$ to $\mathrm{Cl}_{(4)}(k)/\mathrm{Cl}_{(4)}(k)^2$, proving (1).

(2). By Lemmas 3.15 and 3.16 we have $|Z^S_{(2)}/Z^2_{(2)}| = 8/2 = 4$, so by the exact sequence of Proposition 3.13 $|C_{(4)}|$ is equal to $|C_{(1)}|$, $2|C_{(1)}|$, or $4|C_{(1)}|$. However, it cannot be $4|C_{(1)}|$: if it were, by the same exact sequence this would imply that $S^S_{(4)}(k) = S^S(k)$, so that if any $u \in k$, coprime to 2, represents an element of $S^S(k)$, the equation $x^2 \equiv u \pmod{{}^*4}$ is soluble. By Proposition 3.3 this implies that each element of $S^S(k)$ yields a quadratic extension of k of discriminant (1); however, if $|C_{(4)}| > |C_{(1)}|$, then there exist quadratic extensions of k of nontrivial square discriminant dividing (4) and unramified at infinity, hence by Lemma 3.6 generated by virtual units of square norm, a contradiction.

For the second statement, note that the 1^s coefficient of $a(k)2^{r_2(k)}\Phi_k(s)$ is equal to $|C_{(4)}|$. This may be seen from Theorem 3.2, or equivalently, it is a consequence of various computations in this section. This 1^s coefficient counts the number of quadratic or trivial extensions $K_6 = k(\sqrt{\alpha})$, where α is of square norm, and K_6/k is unramified at all finite places.

By (1), $|C_{(1)}|$ counts the number of such extensions K_6/k which are also unramified at infinity. Thus, in the totally real case, $|C_{(4)}| > |C_{(1)}|$ if and only if $\mathrm{rk}_2^+(k) \neq \mathrm{rk}_2(k)$. In the complex case, due to the factor of $2^{r_2(k)} = 2$, we necessarily have $|C_{(4)}| > |C_{(1)}|$.

By the ray class group exact sequence, we have $\mathrm{rk}_2^+(k) = \mathrm{rk}_2(k)$ if and only if $\mathrm{Cl}^+(k) = \mathrm{Cl}(k)$ if and only if $[U(k) : U^+(k)] = 2^{r_1} = [U(k) : U^2(k)]$, and since $U^2(k) \subset U^+(k)$, if and only if $U^+(k) = U^2(k)$, proving our claim.

(3). This follows from the existence of natural surjections $C_{\mathfrak{c}} \longrightarrow C_{\mathfrak{c}'}$ for $\mathfrak{c}'|\mathfrak{c}$. □

The following is independent of the rest of this paper but is an immediate consequence of the above proof. It seems that there should exist a simple direct proof of this corollary, which would provide a simpler proof of (2) above, but we did not find such a proof.

Corollary 4.2. *Let k be a cubic field. There exists a virtual unit u coprime to 2 and of square norm such that $u \not\equiv 1 \pmod{4\mathbb{Z}_k}$.*

Proof. Indeed, since the class of a virtual unit in $S(k)$ can always be represented by a virtual unit coprime to 2, the statement is equivalent to the statement that the natural injection from $S^S_{(4)}(k)$ to $S^S(k)$ is not surjective, and by the exact sequence of Proposition 3.13, that $|C_{(4)}| \neq 4|C_{(1)}|$, proved above. □

In most cases, Proposition 4.1 will suffice to handle the groups $C_{\mathfrak{c}^2}$, but in two special cases where $C_{\mathfrak{c}^2} \simeq C_{(4)}$, we will need to evaluate $\chi(\mathfrak{a})$ for characters $\chi \in X_{\mathfrak{c}^2}$ on ideals $\mathfrak{a}$ which are coprime to $\mathfrak{c}^2$ but not 4. For this we require the following refinement.

Proposition 4.3. *Suppose that $(2) = \mathfrak{c}\mathfrak{c}'$ with $\mathfrak{c}$ and $\mathfrak{c}'$ coprime and squarefree and $\mathcal{N}(\mathfrak{c}') = 4$; namely, either*

- *$(2) = \mathfrak{p}_1\mathfrak{p}_2$ with each $\mathfrak{p}_i$ of degree i, $\mathfrak{c} = \mathfrak{p}_1$, and $\mathfrak{c}' = \mathfrak{p}_2$, or*
- *$(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with each $\mathfrak{p}_i$ of degree 1, $\mathfrak{c} = \mathfrak{p}_1$, and $\mathfrak{c}' = \mathfrak{p}_2\mathfrak{p}_3$.*

Then, the map $\mathfrak{a} \to \mathfrak{a}/\mathcal{N}(\mathfrak{a})$ induces an isomorphism

$$Cl_{\mathfrak{c}'^2}(k)/Cl_{\mathfrak{c}'^2}(k)^2 \xrightarrow{\phi} C_{\mathfrak{c}^2}\ , \tag{4.3}$$

which agrees with (4.2) on ideals coprime to (2), and for which $\phi(\mathfrak{p}_1^2) = 4/\mathfrak{p}_1^2$.

Proof. Because 2 is unramified and $\mathcal{N}(\mathfrak{c}) = 2$, the map $\mathfrak{a} \to \mathfrak{a}/\mathcal{N}(\mathfrak{a})$ sends ideals coprime to $\mathfrak{c}'$ to ideals coprime to $\mathfrak{c}$. The map $\mathfrak{b} \to \mathfrak{b}/\sqrt{\mathcal{N}(\mathfrak{b})}$ does *not* necessarily send ideals coprime to $\mathfrak{c}$ to ideals coprime to $\mathfrak{c}'$, for example if $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{c} = \mathfrak{p}_1$, and $\mathfrak{b} = \mathfrak{p}_2^2$. Therefore a somewhat more subtle argument is required.

We begin with the surjective homomorphism

$$\mathrm{Cl}_{(4)}(k)/\mathrm{Cl}_{(4)}(k)^2 \xrightarrow{\phi} C_{(4)} \twoheadrightarrow C_{\mathfrak{c}^2}\ , \tag{4.4}$$

which we check contains in its kernel all $\alpha \equiv 1 \pmod{{}^*\mathfrak{c}'^2}$: given such an α, $\beta := \alpha/\mathcal{N}(\alpha)$ must be coprime to 2 (the $\mathfrak{p}_1$-adic valuations of α and $\mathcal{N}(\alpha)$ must be equal), and we must

have $\pm\beta \equiv 1 \pmod{{}^*\mathfrak{p}_1^2}$, so that (β) represents the trivial class of $C_{\mathfrak{c}^2}$. Therefore (4.4) induces a surjection

$$\mathrm{Cl}_{\mathfrak{c}'^2}(k)/\mathrm{Cl}_{\mathfrak{c}'^2}(k)^2 \xrightarrow{\widetilde{\phi}} C_{\mathfrak{c}^2}\ , \tag{4.5}$$

which must be an isomorphism because *both groups in* (4.3) *are of the same size*[6]. It coincides with ϕ on ideals coprime to (2), and hence for all ideals, so that $\phi = \widetilde{\phi}$ is the desired isomorphism. □

5 Splitting types in k, K_6, and L

By the results of the previous section, together with class field theory, we can translate characters of $C_{\mathfrak{c}^2}$ into characters of Galois groups of quadratic extensions. It is therefore important to understand the possible ways in which primes can split in k, K_6, and L. The following gives a complete answer to this question:

Theorem 5.1. *Let L be an A_4 or S_4-quartic field, and let k be its cubic resolvent. Suppose first that $p \geq 3$ is a prime number.*

1. *If p is (3) in k, then p is (31) in L.*
2. *If p is (21) in k, then p is (4), (211), (2^2), or (1^21^2) in L.*
3. *If p is (111) in k, then p is (1111), (22), (2^2), or (1^21^2) in L.*
4. *If p is (1^21) in k, then p is (21^2), (1^211), or (1^4) in L.*
5. *If p is (1^3) in k, then p is (1^31) in L.*

If $p = 2$, then in addition to the above decomposition types, in all cases 2 can be (1^4) in L, if 2 is (1^21) in k then 2 can also be (1^21^2) in L, and if 2 is $(1^21)_4$ in k then 2 can also be (2^2) in L.

Moreover, we have the Artin relation

$$\zeta_L(s) = \frac{\zeta(s)\zeta_{K_6}(s)}{\zeta_k(s)} \tag{5.1}$$

among the Dedekind zeta functions associated to L, K_6, k, and $\mathbb{Q}$, allowing us to determine the splitting types of a prime p in any of k, L, and K_6 from the splitting in the remaining two fields.

Theorem 5.1 overlaps substantially with works of Dribin [17], Martinet (unpublished), and Wong [29]. For this reason, and also because our proof involves a long list of *ad hoc* group-theoretic arguments ruling out a variety of individual cases, we give here only an outline of a complete proof. An expanded version of this section with complete proofs is available from the second author's website[7].

Proof. The Eq. (5.1) is a well-known consequence of the character theory of A_4 and S_4, and we omit the details here.

For the first part of the theorem, the basic idea of the proof is as follows: A prime p may have splitting type (3), (21), (111), (1^21), or (1^3) in k, and each of the primes above p may be ramified, split, or inert in K_6; by (5.1), this determines the splitting type of p in L.

[6] This fact is proved in Proposition 8.1, which does not in turn rely on the proposition being proved. We might have waited until Section 8 to give the current proof, but we placed it here for readability's sake.

[7] http://people.math.sc.edu/thornef/.

By computer search, we found triples (k, K_6, L) for each combination of splitting types listed in the theorem. It therefore remains to prove that no other combinations are possible. Several tools useful for this include:

- We can use (5.1) to rule out some combinations, for example, (21) in k and (411) in K_6.
- A theorem of Stickelberger says that if F is a number field of degree n and p is a prime unramified in F which splits into g prime ideals, then $(\mathrm{Disc}(F))p = (-1)^{n-g}$. Thus, since $\mathrm{Disc}(L) = \mathrm{Disc}(k)f(L)^2$, it follows that when p is unramified both in k and L the number of primes above p in k and L must have opposite parity. This rules out, for example, the possibility that p is (21) in k and (222) in K_6.
- Using the square norm condition: recall that $\mathfrak{d}(K_6/k) = 4\mathfrak{a}/\mathfrak{c}^2$ with $\mathfrak{a}$ integral, squarefree, and of square norm. Thus if $\mathfrak{p}$ is a prime ideal of k not dividing 2 which is ramified in K_6/k, we must have $\nu_{\mathfrak{p}}(\mathfrak{a}) = 1$, and a short computation shows that $\sum_{\mathfrak{p}|p\mathbb{Z}_k, \mathfrak{p}|\mathfrak{d}(K_6/k)} f(\mathfrak{p}/p)$ is even. This rules out, for example, the possibility that a prime $p \neq 2$ splits as (21) in k and (221^2) in K_6. This condition does not apply to $p = 2$, and indeed more splitting types are possible for $p = 2$.
- Using divisibility by 3 of ramification degrees: suppose that a prime p splits as $(1^3 1)$ in $L/\mathbb{Q}$. If $\mathfrak{P}$ is a prime of $\widetilde{L}$ above p, the ramification index $e(\mathfrak{P}|p)$ must be divisible by 3, implying that p is (1^3) in k.

This leaves nine additional cases to rule out, which split further into subcases depending on whether L is an S_4 or A_4-quartic field. We accomplished this using a variety of group-theoretic arguments. We give a single example illustrating the flavor of these proofs, and refer to the aforementioned note for proofs for the remaining cases.

- Suppose that p is (21) in k (221^2) in K_6, and (21^2) in L, where L is an S_4-quartic field. Writing $[\widetilde{L} : \mathbb{Q}] = efg$ with the usual meaning, we have $2 \mid e$ and $2 \mid f$. If $\mathfrak{P}$ is an ideal of $\widetilde{L}$ above the ideal $\mathfrak{p}$ of L with $f(\mathfrak{p}|p) = 2$, we have $e(\mathfrak{P}|\mathfrak{p}) \,|\, [\widetilde{L} : L] = 6$, and since $e(\mathfrak{p}|p) = 1$ it follows that $e = e(\mathfrak{P}|p) \mid 6$, so that $e = 2$. Similarly, by considering the ideal $\mathfrak{p}$ of L with $e(\mathfrak{p}|p) = 2$ we see that $f = 2$. Thus the decomposition fields are quartic fields, and since the only quartic subfields of $\widetilde{L}$ are the conjugates of L, it follows that L is a decomposition field, a contradiction since none of the prime ideals $\mathfrak{p}$ of L above p satisfy $e(\mathfrak{p}|p) = f(\mathfrak{p}|p) = 1$.

□

We will also need the following simple consequence of (5.1) in the sequel.

Proposition 5.2. *A prime p is (1^4) in L if and only if all the prime ideals above p in k are ramified in the quadratic extension K_6/k.*

6 The arithmetic of quartic fields in $\mathcal{L}_2(k)$

Recall that in Definition 1.2 we wrote

$$\mathcal{L}_2(k) = \mathcal{L}(k, 1) \cup \mathcal{L}(k, 4) \cup \mathcal{L}(k, 16) \cup \mathcal{L}_{tr}(k, 64) \ .$$

The point of this definition is the following crucial result:

Theorem 6.1. *We have $L \in \mathcal{L}_2(k)$ if and only if the corresponding extension of trivial norm as explained in Theorem 2.2 is of the form $K_6 = k(\sqrt{\beta})$, where $\beta \in V^+(k)$ is coprime to 2.*

Proof. Assume first that $\beta \in V^+(k)$. By Proposition 3.3 and Lemma 3.6 we have $\mathfrak{d}(K_6/k) = 4/\mathfrak{c}^2$, so $\mathcal{N}(\mathfrak{d}(K_6/k)) = \mathrm{Disc}(L)/\mathrm{Disc}(k) = 64/\mathcal{N}(\mathfrak{c})^2$. Since β is totally positive, when k is totally real so are K_6 and the Galois closure of L, so L is totally real. If $\mathfrak{c} \neq \mathbb{Z}_k$ we have $64/\mathcal{N}(\mathfrak{c})^2 = 1$, 4, or 16, so $L \in \mathcal{L}_2(k)$. Thus assume that $\mathfrak{c} = \mathbb{Z}_k$, so that $\mathrm{Disc}(L) = 64\mathrm{Disc}(k)$ and $\mathfrak{d}(K_6/k) = 4$. This implies that all the primes above 2 in k are ramified in K_6/k, so by Proposition 5.2 the prime 2 is totally ramified in L.

Conversely, let $L \in \mathcal{L}_2(k)$ and let $K_6 = k(\sqrt{\alpha})$ be the corresponding extension, where α is of square norm. Write $\alpha\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$, where $\mathfrak{a}$ is unique if we choose it integral and squarefree, and $\mathfrak{q}$ can be chosen coprime to 2. Note that if k is totally real then so is L and hence K_6, so α will automatically be totally positive. Since α has square norm, so does $\mathfrak{a}$. Since $\mathfrak{d}(K_6/k) = 4\mathfrak{a}/\mathfrak{c}^2$ with $\mathfrak{c} \mid 2\mathbb{Z}_k$ coprime to $\mathfrak{a}$ and $\mathcal{N}(\mathfrak{d}(K_6/k)) = \mathrm{Disc}(L)/\mathrm{Disc}(k) = 2^{2j}$ for $0 \leq j \leq 3$, it follows that $\mathfrak{a}$ is a product of distinct prime ideals above 2, whose product of norms is a square. If $\mathfrak{a} = \mathbb{Z}_k$ then $\beta = \alpha$ is a virtual unit coprime to 2. Thus, assume by contradiction that $\mathfrak{a} \neq \mathbb{Z}_k$. Considering the five possible splitting types of 2 in k and using the fact that $\mathcal{N}(\mathfrak{a}) \leq \mathcal{N}(\mathfrak{c}^2)$, it is immediate to see that the only remaining possibilities are as follows:

- $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_2$ of degree 2, $\mathfrak{a} = \mathfrak{p}_2$, $\mathfrak{c} = \mathfrak{p}_1$, $\mathfrak{d}(K_6/k) = \mathfrak{p}_2^3$, hence $L \in \mathcal{L}(k, 64)$. Then $\mathfrak{p}_1$ is not ramified in K_6/k so by Proposition 5.2 2 is not totally ramified in L, a contradiction.
- $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{c} = \mathfrak{p}_3$, $\mathfrak{d}(K_6/k) = (\mathfrak{p}_1\mathfrak{p}_2)^3$, hence $L \in \mathcal{L}(k, 64)$. Similarly, here $\mathfrak{p}_3$ does not ramify in K_6/k, so 2 is not totally ramified in L, again a contradiction and proving the theorem.

□

In light of Lemma 3.6, we immediately obtain the following:

Corollary 6.2. *Suppose that L is an A_4 or S_4-quartic field, with K_6 the corresponding quadratic extension of k. Then $L \in \mathcal{L}_2(k)$ if and only if K_6/k is unramified at infinity and $\mathfrak{d}(K_6/k) | 4\mathbb{Z}_k$.*

The analysis for A_4-quartic fields is greatly simplified by the following result.

Proposition 6.3. *If k is a cyclic cubic field then $rk_2(k)$ is even and $rk_2^+(k) = rk_2(k)$. In addition, if $a \in \mathbb{Z}$, the 2-ranks of $Cl_{a\mathbb{Z}_k}(k)$ and of $Cl^+_{a\mathbb{Z}_k}(k)$ are also even.*

Proof. There is a natural action of the group ring $\mathbb{Z}[G]$ on $\mathrm{Cl}(k)$ and on $\mathrm{Cl}^+(k)$, and in the cyclic cubic case $G = \langle\sigma\rangle$, where $1 + \sigma + \sigma^2$ acts trivially, so we have an action of $\mathbb{Z}[\sigma]/(1 + \sigma + \sigma^2) \simeq \mathbb{Z}[\zeta_3]$. Since 2 is inert in $\mathbb{Z}[\zeta_3]$ it follows that any 2-torsion $\mathbb{Z}[\zeta_3]$-module has even rank, so in particular $\mathrm{rk}_2(k)$ and $\mathrm{rk}_2^+(k)$ are even. Furthermore, by a

theorem of Armitage and Fröhlich [1], for any number field K with r_1 real embeddings we have

$$\mathrm{rk}_2^+(K) \leq \mathrm{rk}_2(K) + \lfloor r_1/2 \rfloor \,, \tag{6.1}$$

so in our case $\mathrm{rk}_2^+(k) \leq \mathrm{rk}_2(k) + 1$, so that we have equality since both ranks are even.

The final statement is true for the same reason as above: the G-invariance of $a\mathbb{Z}_k$ guarantees that $\mathrm{Cl}_{a\mathbb{Z}_k}(k)$ and $\mathrm{Cl}^+_{a\mathbb{Z}_k}(k)$ are also $\mathbb{Z}[\zeta_3]$-modules. □

These results, combined with our previous work (especially Proposition 4.1), imply the following counting formulas:

Proposition 6.4. *The following statements are true:*

1. *We have* $|\mathcal{L}(k,1)| = (2^{rk_2(k)} - 1)/a(k) = (|C_{(1)}| - 1)/a(k)$, *where* $a(k)$ *is as in Definition 1.1.*
2. *We have* $|\mathcal{L}_2(k)| = |C_{(4)}| - 1$, *so that for noncyclic* k, $|\mathcal{L}_2(k)|$ *is equal to either* $|\mathcal{L}(k,1)|$ *or* $2|\mathcal{L}(k,1)| + 1$.
3. *We have* $\mathcal{L}(k,4) = \mathcal{L}(k,16) = \mathcal{L}_{tr}(k,64) = \emptyset$ (*equivalently,* $|\mathcal{L}_2(k)| = |\mathcal{L}(k,1)|$) *if and only if* k *is totally real and* $rk_2^+(k) = rk_2(k)$, *i.e., if and only* k *is totally real and there does not exist a nonsquare totally positive unit. In particular, this is true for cyclic fields.*
4. *If one of* $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, *or* $\mathcal{L}_{tr}(k,64)$ *is nonempty then the other two are empty.*

Proof. (1). By Theorem 2.2, the elements of $\mathcal{L}(k,1)$ are in $a(k)$-to-1 correspondence with the quadratic extensions of k which are unramified everywhere (including at the infinite places). By class field theory, they correspond to subgroups of $\mathrm{Cl}(k)$ of index 2, yielding the first equality. The second equality is a consequence of (1) of Proposition 4.1.

(2). The elements of $\mathcal{L}_2(k)$ may have the ramification described in Corollary 6.2, and the equality again follows by class field theory and Proposition 4.1.

(3). This follows from (2) of Proposition 4.1: the latter criterion is equivalent to the equality $|C_{(4)}| = |C_{(1)}|$. The statement for cyclic fields follows from Proposition 6.3.

(4) If $|C_{(4)}| \neq |C_{(1)}|$, then $|\mathrm{Cl}_4(k)[2]\,| = 2|\mathrm{Cl}(k)[2]\,|$. Among the ideals dividing (4), choose a minimal ideal $\mathfrak{m}$ with the property that $|\mathrm{Cl}_{\mathfrak{m}}(k)[2]\,| = 2|\mathrm{Cl}(k)[2]\,|$. Then $\mathfrak{m}$ must be a square by Lemma 3.6, and all extensions K_6/k counted by $\mathrm{Cl}_{(4)}(k)[2]$ must have $\mathfrak{d}(K_6/k) = \mathbb{Z}_k$ or $\mathfrak{d}(K_6/k) = \mathfrak{m}$. Therefore, all of the fields in $\mathcal{L}_2(k)$ have discriminant equal to either $\mathrm{Disc}(k)$ or $\mathrm{Disc}(k) \cdot \mathcal{N}(\mathfrak{m})$, with $\mathcal{N}(\mathfrak{m})$ equal to 4, 16, or 64. □

In Section 7 we prove further results about the arithmetic of S_4-quartic fields in particular. We conclude this section with the following result, which is an analogue for A_4-quartic fields of a related result in [14]. As with that proposition the result is not required elsewhere in this paper; rather, it is an application of Theorem 1.4 (2).

Proposition 6.5. *Let* k *be a cyclic cubic field such that* $rk_2(k) = 4$, *so that there exist five* A_4*-quartic fields* L *with cubic resolvent* k, *which all satisfy* $Disc(L) = Disc(k)$. *If 2 is totally*

split in k, then 2 is totally split in exactly one of the five A_4-quartic fields L, and splits as $2\mathbb{Z}_L = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_i$ of degree 2 in the four others.

Proof. Writing $D = \mathrm{Disc}(k)$, we use Theorem 1.4 (2) to count the number of cubic fields of discriminant D, $16D$, $64D$, and $256D$. By hypothesis (and Proposition 6.3), $\mathrm{rk}_2(\mathrm{Cl}(k)) = \mathrm{rk}_2(\mathrm{Cl}^+(k)) = 4$.

Write $5 = a + b$, where of the five quartic fields L, 2 is totally split in a of them, and 2 is (22) in b of them. By Theorem 5.1 these are no other possibilities, and we prove that $a = 1$.

The $1^{-s}, 2^{-s}, 4^{-s}, 8^{-s}$, and 16^{-s} coefficients of $\Phi_k(s)$ are equal to $\frac{16}{3}, 0, 16, 8a-8, 8a-8$ respectively. Therefore, the number of quadratic extensions K_6/k, ramified only at infinity and/or 2, is equal to $3\big(-\frac{1}{3}+\frac{16}{3}+16+2\cdot(8a-8)\big) = 15+48a$. These extensions, together with the trivial extension k/k, are counted by the ray class group $\mathrm{Cl}^+_{(8)}(k)/\mathrm{Cl}^+_{(8)}(k)^2$. By Proposition 6.3, this has even 2-rank. Hence, $16 + 48a = 2^r$ where $r \geq 6$ is even. (We know that $r \neq 4$ because the 4^{-s} coefficient is nonzero).

In addition to $a = 1$ and $r = 6$, this equation also has one other solution $a = 5$ and $r = 8$, and we conclude the proof by ruling this out. Consider the ray class group exact sequence ([6] Proposition 3.2.3)

$$1 \to U^+_{(n)}(k) \to U(k) \to (\mathbb{Z}_k/n\mathbb{Z}_k)^\times \times \mathbb{F}_2^3 \to \mathrm{Cl}^+_{(n)}(k) \to \mathrm{Cl}(k) \to 1\,, \tag{6.2}$$

for $n = 1$ and $n = 8$. (Here $U^+_{(n)}(k)$ is the group of totally positive units congruent to 1 (mod $^*n$).) As $\mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2 \simeq \mathrm{Cl}(k)/\mathrm{Cl}(k)^2$, we know that the image of $U(k)$ surjects onto $\mathbb{F}_2^3$, i.e., that all eight sign signatures are represented by units of k. Since $(\mathbb{Z}_k/8\mathbb{Z}_k)^\times$ has 2-rank 3 (recall that 2 is totally split), this implies that $\mathrm{rk}_2(\mathrm{Cl}^+_{(8)}(k)) \leq \mathrm{rk}_2(\mathrm{Cl}(k))+3 = 4+3 = 7$. Therefore $r \neq 8$ and the proof is complete. □

Remark. It ought to be possible to prove similar statements for related situations (e.g. if $\mathrm{rk}_2(k) = 6$), but we have not pursued this.

7 The arithmetic of S_4-quartic fields in $\mathcal{L}_2(k)$

In this section we further study the set $\mathcal{L}_2(k)$ in the (more complicated) S_4 case. If k is an S_3-cubic field, then by Proposition 6.4, at most one of $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, and $\mathcal{L}_{tr}(k,64)$ can be nonempty. We will prove the following:

Proposition 7.1. *Let k be an S_3-cubic field and let $L \in \mathcal{L}_2(k)$. Then the following table gives a complete list of all possibilities for the following data:*

- *The splitting type of 2 in k, K_6, and L, and if it is $(1^2 1)$ in k we also include as a subscript Disc(k) (mod 8);*
- *The quantity $n^2 := \mathrm{Disc}(L)/\mathrm{Disc}(k)$, which must be equal to 1, 4, 16, or 64.*

For each possible combination we give a cubic polynomial generating k over $\mathbb{Q}$, the characteristic polynomial $P_\alpha(x)$ of α of square norm such that $K_6 = k(\sqrt{\alpha})$, and a defining polynomial for L over $\mathbb{Q}$.

k-split	K_6-split	L-split	n^2	k	$P_\alpha(x)$	L
(3)	(33)	(31)	1	$x^3-x^2-14x+23$	$x^3-35x^2+179x-81$	$x^4-x^3-4x^2+x+2$
(3)	(3^2)	(1^4)	64	x^3-x^2-4x+3	$x^3-15x^2+55x-49$	$x^4-2x^3-6x^2+2$
(21)	(42)	(4)	1	$x^3-x^2-9x+10$	$x^3-8x^2+12x-1$	x^4-4x^2-x+1
(21)	(2211)	(211)	1	$x^3-20x-17$	$x^3-12x^2+28x-1$	x^4-6x^2-x+2
(21)	(2^22)	(2^2)	16	$x^3-x^2-14x-4$	$x^3-22x^2+21x-4$	$x^4-11x^2-2x+25$
(21)	(2^211)	(1^21^2)	16	x^3-x^2-7x+6	$x^3-13x^2+36x-16$	$x^4-2x^3-5x^2+2x+2$
(21)	(2^21^2)	(1^4)	64	x^3-4x-1	$x^3-11x^2+19x-1$	$x^4-2x^3-4x^2+4x+2$
(111)	(2211)	(22)	1	$x^3-x^2-34x-16$	$x^3-67x^2+947x-625$	$x^4-x^3-8x^2+x+3$
(111)	(21^21^2)	(2^2)	16	$x^3-13x-4$	$x^3-14x^2+45x-4$	x^4-7x^2-2x+1
(111)	(111111)	(1111)	1	$x^3+x^2-148x+480$	$x^3-37x^2+308x-576$	$x^4-2x^3-17x^2-6x+16$
(111)	(1^21^211)	(1^21^2)	16	$x^3-17x-8$	$x^3-26x^2+65x-36$	$x^4-13x^2-6x+26$
(111)	$(1^21^21^2)$	(1^4)	—	—	—	—
$(1^21)_0$	(2^211)	(21^2)	1	$x^3-x^2-18x-14$	$x^3-43x^2+323x-25$	$x^4-x^3-5x^2+2x+2$
$(1^21)_0$	(1^21^211)	(1^211)	1	$x^3-x^2-58x+186$	$x^3-75x^2+499x-169$	$x^4-x^3-9x^2+3x+14$
$(1^21)_0$	(1^411)	(1^21^2)	4	$x^3-22x-8$	$x^3-14x^2+25x-4$	x^4-7x^2-2x+6
$(1^21)_0$	(1^41^2)	(1^4)	64	x^3-x^2-6x+2	$x^3-16x^2+60x-16$	x^4-8x^2-4x+1
$(1^21)_4$	(2^211)	(21^2)	1	$x^3-x^2-20x-22$	$x^3-43x^2+291x-121$	$x^4-x^3-5x^2+4x+2$
$(1^21)_4$	(1^21^211)	(1^211)	1	$x^3-59x-168$	$x^3-91x^2+915x-1849$	$x^4-x^3-11x^2+11x+16$
$(1^21)_4$	(1^42)	(2^2)	4	$x^3-11x-12$	$x^3-10x^2+21x-4$	x^4-5x^2-2x+1
$(1^21)_4$	(1^42)	(2^2)	16	$x^3-x^2-8x+10$	$x^3-13x^2+32x-16$	$x^4-2x^3-5x^2+2x+3$
$(1^21)_4$	(1^411)	(1^21^2)	16	$x^3-22x-20$	$x^3-17x^2+64x-16$	$x^4-2x^3-7x^2+4x+2$
$(1^21)_4$	(1^41^2)	(1^4)	—	—	—	—
(1^3)	(1^31^3)	(1^31)	1	$x^3-x^2-27x-43$	$x^3-43x^2+179x-9$	$x^4-x^3-5x^2+3x+4$
(1^3)	(1^6)	(1^4)	4	$x^3-x^2-9x+11$	$x^3-12x^2+16x-4$	x^4-6x^2-2x+5
(1^3)	(1^6)	(1^4)	64	x^3-x^2-7x-3	$x^3-20x^2+104x-144$	$x^4-10x^2-12x-1$

Remarks 7.2.
- The empty rows in the table correspond to combinations not ruled out for $p=2$ in the table in Theorem 5.1, but which we will prove cannot occur for $L\in\mathcal{L}_2(k)$.
- In each case we have chosen the noncyclic totally real cubic field k with smallest discriminant satisfying the given splitting conditions for k, L, and value of $n^2=\mathrm{Disc}(L)/\mathrm{Disc}(k)$, and in addition such that $|\mathcal{L}_2(k)|\le 1$. One could also in most cases also choose complex cubic fields if desired.
- We could simplify this table by giving in addition to the splittings, only the $P_\alpha(x)$ column, since P_α also generates the field k, the field K_6 is given by the polynomial $P_\alpha(x^2)$, and the field L by Proposition 2.3. We have preferred to keep it as above.
- As with Theorem 5.1, our results in this section partially overlap with unpublished work of Martinet.

In particular, the above proposition and table implies that for the S_4 case, the table of Theorem 1.4 covers precisely the cases that occur. For the A_4 case this is easy to check using Theorem 5.1 alone.

Most of Proposition 7.1 is contained within the following:

Proposition 7.3. *Let k be a cubic field such that either k is complex, or k is totally real and $rk_2^+(k) > rk_2(k)$, so that by Proposition 6.4, one and exactly one of $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, or $\mathcal{L}_{tr}(k,64)$ is nonempty. Denote temporarily by $W^+(k)$ the group of $u\in V^+(k)$ coprime to 2, and by $W^+_{(4)}(k)$ the group of $u\in W^+(k)$ such that $x^2\equiv u \pmod{{}^*(4)}$ is soluble (equivalently, $\overline{u}\in S^+_{(4)}(k)$).*

(1) If 2 is (3) *in k, then $\mathcal{L}_{tr}(k,64)\neq\emptyset$.*

(2) *If 2 is* (21) *in k, write* $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ *with* $\mathfrak{p}_i$ *of degree i. Then if* $v_{\mathfrak{p}_1}(\alpha - 1) = 1$ *for some* $\alpha \in W^+(k)$ *we have* $\mathcal{L}(k, 16) = \emptyset$ *and* $\mathcal{L}_{tr}(k, 64) \neq \emptyset$*, while if* $v_{\mathfrak{p}_1}(\alpha - 1) \geq 2$ *for some* $\alpha \in W^+(k) \setminus W^+_{(4)}(k)$ *the reverse is true.*

(3) *If 2 is* (111) *in k then* $\mathcal{L}(k, 16) \neq \emptyset$*.*

(4) *If 2 is* $(1^21)_0$ *in k, write* $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$*. Then if* $v_{\mathfrak{p}_1}(\alpha - 1) = 1$ *for some* $\alpha \in W^+(k)$ *we have* $\mathcal{L}(k, 4) = \emptyset$ *and* $\mathcal{L}_{tr}(k, 64) \neq \emptyset$*, while if* $v_{\mathfrak{p}_1}(\alpha - 1) \geq 2$ *for some* $\alpha \in W^+(k) \setminus W^+_{(4)}(k)$ *the reverse is true.*

(5) *If 2 is* $(1^21)_4$ *in k, write* $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$*. Then if* $v_{\mathfrak{p}_1}(\alpha - 1) = 1$ *for some* $\alpha \in W^+(k)$ *we have* $\mathcal{L}(k, 4) = \emptyset$ *and* $\mathcal{L}(k, 16) \neq \emptyset$*, while if* $v_{\mathfrak{p}_1}(\alpha - 1) \geq 2$ *for some* $\alpha \in W^+(k) \setminus W^+_{(4)}(k)$ *the reverse is true.*

(6) *If 2 is* (1^3) *in k, write* $2\mathbb{Z}_k = \mathfrak{p}_1^3$*. Then if* $v_{\mathfrak{p}_1}(\alpha - 1) = 1$ *for some* $\alpha \in W^+(k)$ *we have* $\mathcal{L}(k, 4) = \emptyset$ *and* $\mathcal{L}_{tr}(k, 64) \neq \emptyset$*, while if* $v_{\mathfrak{p}_1}(\alpha - 1) \geq 2$ *for some* $\alpha \in W^+(k) \setminus W^+_{(4)}(k)$ *the reverse is true.*

Remarks 7.4.

- The conditions in each of the cases (2), (4), (5), (6) are mutually exclusive, and where we write "while ... the reverse is true", it is indeed for *some* $\alpha \in W^+(k) \setminus W^+_{(4)}(k)$ (it is also true if one replaces "some" by "all"). In particular, if α and β in $W^+(k)$ are such that $v_{\mathfrak{p}_1}(\alpha - 1) = 1$ and $v_{\mathfrak{p}_1}(\beta - 1) \geq 2$, we have necessarily $\beta \in W^+_{(4)}(k)$, since otherwise this would contradict the fact that only one of $\mathcal{L}(k, 4)$, $\mathcal{L}(k, 16)$, and $\mathcal{L}_{tr}(k, 64)$ is nonempty.
- We can further rephrase the conditions on α as follows. Let (α_i) be an $\mathbb{F}_2$-basis for $W^+(k)/k^{*2} = V^+(k)/k^{*2} = S^+(k)$, chosen so that each α_i is coprime to 2. Then, for any prime $\mathfrak{p}$ over 2, $v_{\mathfrak{p}}(\alpha - 1) = 1$ for some $\alpha \in W^+(k)$ if and only if it is true for one of the α_i.
  To prove the nontrivial direction of this we use the equality

$$(\alpha - 1)(\alpha' - 1) = (\alpha\alpha' - 1) - (\alpha + \alpha' - 2)\,, \tag{7.1}$$

  so that whenever $v_{\mathfrak{p}}(\alpha - 1) \geq 2$ and $v_{\mathfrak{p}}(\alpha' - 1) \geq 2$, then $v_{\mathfrak{p}}(\alpha + \alpha' - 2) \geq 2$ and so $v_{\mathfrak{p}}(\alpha\alpha' - 1) \geq 2$.

Before beginning the proof of Proposition 7.3, we collect some useful facts about discriminants.

Proposition 7.5. *Let k be a cubic field, write* $Disc(k) = Df^2$ *with D a fundamental discriminant, and let p be a prime.*

(1) *If* $p \neq 3$ *we have* $v_p(f) \leq 1$ *and* $p \nmid \gcd(D, f)$*.*

(2) *We have* $v_3(f) \leq 2$*, and if* $v_3(f) = 1$ *then* $3 \mid D$*.*

(3) *p is totally ramified in k if and only if* $p \mid f$*.*

(4) *p is partially ramified in k if and only if* $p \mid D$ *and* $p \nmid f$*.*

Proof. This is classical, and we refer to (Section 10.1.5 of [6]) for a proof, except for (2) which can be easily deduced from loc. cit. Note that the last statement of (2) is true but empty for cyclic cubic fields since we have $v_3(f) = 0$ or 2. □

Proposition 7.6. *If k is a cubic field then 2 is (1^3) in k if and only if $Disc(k) \equiv 20 \pmod{32}$, and $(1^2 1)$ if and only if $Disc(k) \equiv 8$ or $12 \pmod{16}$. In particular we have $v_2(Disc(k)) \leq 3$, and we cannot have $Disc(k) \equiv 4 \pmod{32}$.*

Proof. We could prove this by appealing to the Jones-Roberts database of local fields [21], as we will do in similar situations later, but here we prefer to give a simple direct argument. We have $\mathrm{Disc}(k) = Df^2$ for D a fundamental discriminant, and by Proposition 7.5 we cannot have $p^2 \mid f$ or $p \mid \gcd(D,f)$ unless possibly $p = 3$. Thus if f is even we must have $2 \nmid D$ so then $v_2(Df^2) = 2$, while if f is odd we have $v_2(Df^2) = v_2(D) \leq 3$.

By Proposition 7.5 the prime 2 is totally ramified if and only if $2 \mid f$. If this happens, since $2^2 \nmid f$ we can write $f = 2f_1$ with f_1 odd, so $f^2 = 4f_1^2 \equiv 4 \pmod{32}$. On the other hand, D is an odd fundamental discriminant, so $D \equiv 1 \pmod 4$, so it follows already that $Df^2 \equiv 4 \pmod{16}$. We claim that we cannot have $D \equiv 1 \pmod 8$. This is in fact a result of class field theory: if $D \equiv 1 \pmod 8$ then 2 is split in $K_2 = \mathbb{Q}(\sqrt{D})$ as $2\mathbb{Z}_{K_2} = \mathfrak{p}_1\mathfrak{p}_2$, so $\mathfrak{p}_i \mid f$, which is the conductor of the cyclic cubic extension $\widetilde{k}/K_2$, so by Proposition 3.3.18 of [6], since $\mathcal{N}(\mathfrak{p}_i) = 2$ we have $\mathfrak{p}_i^2 \mid f$, in other words $4 \mid f$, a contradiction which proves our claim.

On the other hand, if 2 is partially ramified we have f odd so $f^2 \equiv 1 \pmod 8$, and D even, so $D \equiv 8$ or $12 \pmod{16}$, so $Df^2 \equiv 8$ or $12 \pmod{16}$. □

Lemma 7.7. *Let L be a quartic field. If 2 is unramified in L then $v_2(Disc(L)) = 0$, and otherwise:*

- *If 2 splits as $(1^2 11)$ or $(1^2 2)$ in L then $v_2(Disc(L)) = 2$ or 3.*
- *If 2 splits as $(1^2 1^2)$ in L then $v_2(Disc(L)) = 4, 5$, or 6.*
- *If 2 splits as $(1^3 1)$ in L then $v_2(Disc(L)) = 2$.*
- *If 2 splits as (2^2) in L then $v_2(Disc(L)) = 4$ or 6.*
- *If 2 splits as (1^4) in L then $v_2(Disc(L)) = 4, 6, 8, 9, 10$, or 11.*

Proof. The étale algebra $L \otimes \mathbb{Q}_2$ splits into one or more extensions of $\mathbb{Q}_2$ of degrees totaling to 4, and $v_2(\mathrm{Disc}(L))$ is the sum of the 2-adic valuations of the discriminants of these extensions. The Jones-Roberts database [21] lists all such extensions of $\mathbb{Q}_2$, reducing the proof to a simple finite computation. □

Proof of Proposition 7.3. We assume below that one of $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, or $\mathcal{L}_{tr}(k,64)$ contains at least one field L, corresponding to an extension $K_6 = k(\sqrt{\alpha})$ which is ramified for at least one prime over 2 (abbreviated below to "is ramified at 2"). By Theorem 6.1 we can choose $\alpha \in W^+(k)$ and $\mathfrak{d}(K_6/k) = 4/\mathfrak{c}^2$ for the largest $\mathfrak{c} \mid (2)$ such that we can solve $\alpha \equiv x^2 \pmod{{}^*\mathfrak{c}^2}$, and since $L \notin \mathcal{L}(k,1)$ we have $\mathfrak{c} \neq (2)$, so with the notation of the proposition $\alpha \notin W^+_{(4)}(k)$.

Lemma 7.8. *Let $\mathfrak{p} \mid (2)$ be a prime ideal, $\alpha \in W(k)$ such that $v_{\mathfrak{p}}(\alpha - 1) = 1$, and $\mathfrak{c}$ the corresponding ideal as above. We then have $\mathfrak{p} \nmid \mathfrak{c}$.*

Proof. Assume on the contrary that $\mathfrak{p} \mid \mathfrak{c}$, so that $v_{\mathfrak{p}}(\alpha - x^2) \geq 2$ for some x. We would then have $v_{\mathfrak{p}}(1 - x^2) = 1$, but either $v_{\mathfrak{p}}(1 - x) = v_{\mathfrak{p}}(1 + x) = 0$, or $v_{\mathfrak{p}}(1 - x) \geq 1$ and $v_{\mathfrak{p}}(1 + x) \geq 1$, in both cases leading to a contradiction. □

Thus the condition $\nu_{\mathfrak{p}}(\alpha - 1) = 1$ implies *a priori* that one of $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, or $\mathcal{L}_{tr}(k,64)$ is nonempty, and in our case-by-case analysis we will use the fact that $\mathfrak{p} \nmid \mathfrak{c}$ to help determine which.

(1). Suppose that 2 is inert. Since $\mathfrak{c} \neq (2)$ we have then $\mathfrak{c} = (1)$, so $\mathcal{N}(\mathfrak{d}(K_6/k)) = 64$, i.e., $L \in \mathcal{L}(k,64)$, hence $L \in \mathcal{L}_{tr}(k,64)$ by Theorem 6.1.

(2) Suppose that $2 = \mathfrak{p}_1\mathfrak{p}_2$ is partially split in k with $\mathfrak{p}_i$ of degree i.

If $\nu_{\mathfrak{p}_1}(\alpha - 1) = 1$, then $\mathfrak{p}_1 \nmid \mathfrak{c}$ by the above lemma. We must also have $\mathfrak{p}_2 \nmid \mathfrak{c}$: Otherwise, we would have $\mathfrak{c} = \mathfrak{p}_2$, hence $\mathcal{N}(\mathfrak{d}(K_6/k)) = 4$, so that $\nu_2(\mathrm{Disc}(L)) = 2$; however, Theorem 5.1 implies that 2 is (2^2), $(1^2 1^2)$, or (1^4) in L, and by Lemma 7.7 there is no such quartic field for which $\nu_2(\mathrm{Disc}(L)) = 2$. Therefore $\mathcal{L}_{tr}(k,64) \neq \emptyset$.

If instead $\nu_{\mathfrak{p}_1}(\alpha - 1) \geq 2$ then $\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_1^2}$ so $\mathfrak{p}_1 | \mathfrak{c}$. Since $\alpha \notin W^+_{(4)}(k)$ we must have $\mathfrak{p}_2 \nmid \mathfrak{c}$, hence $\mathfrak{c} = \mathfrak{p}_1$, and so $\mathcal{L}(k,16) \neq 0$.

(3) Suppose that $2 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ is totally split in k. Since $L \notin \mathcal{L}(k,1)$, at least one of the primes above 2 must ramify in K_6. By Theorem 5.1, 2 must be (2^2), $(1^2 1^2)$, or (1^4) in L, and as above Lemma 7.7 implies that no such field L has $\nu_2(\mathrm{Disc}(L)) = 2$, so that $\mathcal{L}(k,4) = \emptyset$.

Since α can be chosen integral and coprime to 2 and the $\mathfrak{p}_i$ have degree 1, we have $\alpha \equiv 1 \pmod{\mathfrak{p}_i}$ for each i, hence $\alpha = 1 + 2\beta$ for some $\beta \in \mathbb{Z}_k$. We claim that β cannot also be coprime to 2: indeed, if that were the case, we would in turn have $\beta = 1 + 2\gamma$, hence $\alpha = 3 + 4\gamma$, so $\mathcal{N}(\alpha) \equiv 3 \pmod 4$, a contradiction since α has square norm. Thus some $\mathfrak{p}_i$, say $\mathfrak{p}_1$ divides β, hence $\nu_{\mathfrak{p}_1}(\alpha - 1) \geq 2$ so that $\mathfrak{p}_1 \mid \mathfrak{c}$. We cannot have $\mathfrak{c} = \mathfrak{p}_1\mathfrak{p}_j$ for some j since otherwise $\mathcal{L}(k,4)$ would not be empty, nor $\mathfrak{c} = (2)$ since $\alpha \notin W^+_{(4)}(k)$, so that $\mathfrak{c} = \mathfrak{p}_1$ hence $\mathcal{L}(k,16) \neq \emptyset$.

(4). Suppose that $2 = \mathfrak{p}_1^2\mathfrak{p}_2$ is partially ramified with $\mathrm{Disc}(k) \equiv 0 \pmod 8$, so by Lemma 7.6 we have $\nu_2(\mathrm{Disc}(k)) = 3$. Since Lemma 7.7 implies that there is no quartic field L with $\nu_2(\mathrm{Disc}(L)) = 7$, it follows that $\mathcal{L}(k,16) = \emptyset$. In particular we cannot have $\mathfrak{c} = \mathfrak{p}_1$ or $\mathfrak{c} = \mathfrak{p}_2$.

If $\nu_{\mathfrak{p}_1}(\alpha - 1) = 1$, then again $\mathfrak{p}_1 \nmid \mathfrak{c}$ for the corresponding K_6, and we also have $\mathfrak{p}_2 \nmid \mathfrak{c}$ (otherwise $\mathfrak{c} = \mathfrak{p}_2$) so $\mathcal{L}_{tr}(k,64) \neq \emptyset$.

If $\nu_{\mathfrak{p}_1}(\alpha - 1) \geq 2$, then $\mathfrak{p}_1 | \mathfrak{c}$. We cannot have $\mathfrak{p}_1^2 \nmid \mathfrak{c}$ and $\mathfrak{p}_2 \nmid \mathfrak{c}$ since otherwise $\mathfrak{c} = \mathfrak{p}_1$. Since $\alpha \notin W^+_{(4)}(k)$ we thus have $\mathfrak{c} = \mathfrak{p}_1^2$ or $\mathfrak{p}_1\mathfrak{p}_2$, so $\mathcal{L}(k,4) \neq \emptyset$.

(5). Suppose that $2 = \mathfrak{p}_1^2\mathfrak{p}_2$ is partially ramified with $\mathrm{Disc}(k) \equiv 4 \pmod 8$. We use here some results from Section 3. By Definition 3.1 (more precisely Theorem 3.20), we have $z_k(\mathfrak{p}_2) = 2$, so by Lemma 3.15 we have $|Z^S_{\mathfrak{p}_2}/Z^2_{\mathfrak{p}_2}| = 1$, hence by the exact sequence of Proposition 3.13 we deduce that $S^S_{\mathfrak{p}_2^2}(k) = S^S(k)$. By definition of $\mathfrak{c}$ this implies that $\mathfrak{p}_2 \mid \mathfrak{c}$.

If $\nu_{\mathfrak{p}_1}(\alpha - 1) = 1$, then $\mathfrak{p}_1 \nmid \mathfrak{c}$ so $\mathfrak{c} = \mathfrak{p}_2$ and $\mathcal{L}(k,16) \neq \emptyset$. If $\nu_{\mathfrak{p}_1}(\alpha - 1) \geq 2$, then $\mathfrak{p}_1 | \mathfrak{c}$, so since $\alpha \notin W^+_{(4)}(k)$ we have $\mathfrak{c} = \mathfrak{p}_1\mathfrak{p}_2$, hence $\mathcal{L}(k,4) \neq \emptyset$.

(6). Suppose that $2 = \mathfrak{p}^3$ is totally ramified. If $\nu_{\mathfrak{p}}(\alpha - 1) = 1$, then $\mathfrak{p} \nmid \mathfrak{c}$ so $\mathfrak{c} = (1)$ and $\mathcal{L}_{tr}(k,64) \neq \emptyset$. Thus assume that $\nu_{\mathfrak{p}}(\alpha - 1) \geq 2$. We first claim that there exists $\gamma \in k^*$ such that $\nu_{\mathfrak{p}}(\alpha\gamma^2 - 1) \geq 3$. Indeed, set $\gamma = 1 + \pi u$, where π is a uniformizer of $\mathfrak{p}$ and u is 2-integral. We have $\gamma^2 = 1 + 2\pi u + \pi^2 u^2 \equiv 1 + \pi^2 u^2 \pmod{\mathfrak{p}^4}$, so $\nu_{\mathfrak{p}}(\alpha\gamma^2 - 1) \geq 3$ is equivalent to $u^2 \equiv (1/\alpha - 1)/\pi^2 \pmod{\mathfrak{p}}$ which has a solution (for instance $u = (1/\alpha - 1)/\pi^2$), proving our claim. We now claim that for any β of square norm and coprime to 2 (such as $\alpha\gamma^2$), we cannot have $\nu_{\mathfrak{p}}(\beta - 1) = 3$: Indeed, assume this is the case, so that $\beta = 1 + 2\nu$ with ν coprime to 2. By expanding we see that $\mathcal{N}(\beta) \equiv 1 + 2\mathrm{Tr}(\nu) \pmod 4$. As in the proof of Theorem 3.20, we note that the different $\mathfrak{D}(k)$ is divisible by $\mathfrak{p}^2$, so that $\mathfrak{p} = 2\mathfrak{p}^{-2} \subset 2\mathfrak{D}^{-1}(k)$, hence $2 \mid \mathrm{Tr}(w)$ for any $w \in \mathfrak{p}$. Since

ν is coprime to 2 we have $\nu = 1 + w$ with $w \in \mathfrak{p}$, so we deduce that $\mathrm{Tr}(\nu)$ is odd, hence that $\mathcal{N}(\beta) \equiv 3 \pmod 4$, contradicting the fact that β has square norm and proving our claim. It follows that $v_{\mathfrak{p}}(\alpha\gamma^2 - 1) \geq 4$, so that $\mathfrak{p}^2 \mid \mathfrak{c}$, and since $\alpha \notin W^+_{(4)}(k)$ we have $\mathfrak{c} = \mathfrak{p}^2$, so $\mathcal{L}(k,4) \neq 0$. □

Proof of Proposition 7.1. The possibilities listed for $L \in \mathcal{L}(k,1)$ (i.e., with $n^2 = 1$) are precisely those corresponding to the possibilities allowed by the table in Theorem 5.1. In particular we must have K_6/k unramified, and for each row not ruled out we found an example by computer search.

For $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, and $\mathcal{L}_{tr}(k,64)$, we may rule out the following possibilities because they correspond to K_6/k unramified: $k = (3), L = (31)$; $k = (21), L = (4), (211)$; $k = (111), L = (22), (1111)$; $k = (1^21), L = (1^211), (21^2)$; $k = (1^3), L = (1^31)$. Also, for each splitting type in k we rule out columns as in Proposition 7.3.

By definition, we can rule out all possibilities for $\mathcal{L}_{tr}(k,64)$ for which 2 is not (1^4) in L.

We can rule out additional possibilities based on discriminant mismatches. Note that $\mathfrak{d}(K_6/k) = 4/\mathfrak{c}^2$ for some $\mathfrak{c} \mid (2)$, so that if a prime ideal $\mathfrak{p}$ of k ramifies in K_6/k we have $\mathfrak{p}^2 \mid \mathfrak{d}(K_6/k)$, hence the product of $\mathcal{N}(\mathfrak{p})^2$ over all $\mathfrak{p}$ ramified in K_6/k divides $\mathcal{N}(\mathfrak{d}(K_6/k)) = \mathrm{Disc}(L)/\mathrm{Disc}(k)$. For example, suppose that 2 is (111) in k and (1^4) in L. By Theorem 5.1, 2 must be $(1^21^21^2)$ in K_6, so $64 \mid N(\mathfrak{d}(K_6/k))$, in other words $L \in \mathcal{L}_{tr}(k,64)$, contradicting Proposition 7.3 which tells us that $L \in \mathcal{L}(k,16)$.

Variants of this argument rule out the following cases: $k = (21), L = (1^4), L \in \mathcal{L}(k,16)$; $k = (1^21), L = (1^4), L \in \mathcal{L}(k,4)$.

If $k = (1^21)_4, L = (1^4), L \in \mathcal{L}(k,16)$, we have $\mathrm{Disc}(L) = 16 \cdot \mathrm{Disc}(k) \equiv 3 \cdot 2^6 \pmod{2^8}$ by Proposition 7.6. However, by the Jones-Roberts database, there are three totally ramified quartic $L_v/\mathbb{Q}_2$ with $v_2(\mathrm{Disc}(L_v)) = 6$, and they all three satisfy $\mathrm{Disc}(L_v) \equiv 2^6 \pmod{2^8}$. (The discriminant of L_v is defined up to squares of 2-adic units, so that this equation is well-defined.) Therefore we cannot have $L \otimes \mathbb{Q}_2 \simeq L_v$ so this case is impossible.

If $k = (1^21)_4, L = (1^21^2), L \in \mathcal{L}(k,4)$, we have $\mathrm{Disc}(L) \equiv 48 \pmod{64}$ by Proposition 7.6. However, since 2 is (1^21^2) in L, then $L \otimes \mathbb{Q}_2$ is a product of two quadratic extensions of $\mathbb{Q}_2$, each of whose discriminants must have 2-adic valuation 2 (since $v_2(\mathrm{Disc}(L)) = 4$), and therefore (by the local analogue of Proposition 7.6, or again by the Jones–Roberts database which here is trivial) each of whose discriminants must be $12 \pmod{16}$. Therefore, $\mathrm{Disc}(L) \equiv (12 \bmod 16) \cdot (12 \bmod 16) \equiv 16 \pmod{64}$, contradicting the above.

The cases not ruled out above can all happen; to prove this we found the examples listed in the table by computer search. □

8 Proof of Theorem 1.4

We begin with Theorem 3.2, which gave an expression for $\Phi_k(s)$ as a sum involving the product $F_k(\chi, s)$, defined in (3.1) by

$$F_k(\chi,s) = \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2} \left(1 + \frac{\chi(\mathfrak{p}_2)}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2)}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2) + \chi(\mathfrak{p}_1\mathfrak{p}_3) + \chi(\mathfrak{p}_2\mathfrak{p}_3)}{p^s}\right), \tag{8.1}$$

It remains to explicitly evaluate and sum the contributions of $F_k(\chi, s)$ for each $\mathfrak{c}$ and χ. We begin by evaluating the contribution of the trivial characters, which is straightforward.

To handle the nontrivial characters, we must apply Propositions 4.1 and 4.3 to reinterpret them as characters of class groups, and class field theory to further reinterpret them as characters of Galois groups, after which we can evaluate the $\chi(\mathfrak{p}_i)$ in terms of the splitting of $\mathfrak{p}_i$ in quadratic extensions K_6 of k, which (5.1) relates to the splitting of p in the associated quartic extensions $L/\mathbb{Q}$.

We are then ready to evaluate the contributions of the nontrivial characters. When $|C_{(4)}| = |C_{(1)}|$, which includes the A_4 case, this is quite straightforward. When $|C_{(4)}| > |C_{(1)}|$, we must determine the set of $\mathfrak{c}|(2)$ for which $|C_{\mathfrak{c}^2}| = |C_{(4)}|$; this relies on our work in Section 7 and we carry out the computation in Proposition 8.1. In either case, our evaluation of these contributions yields the formulas of Theorem 1.4 and finishes the proof.

8.1 Evaluating the contribution of the trivial characters

The contribution of the trivial characters is equal to

$$\frac{S(s)}{2^{r_2(k)}} \prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2,\, p\neq 2} \left(1+\frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k=\mathfrak{p}_1^2\mathfrak{p}_2,\, p\neq 2} \left(1+\frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\, p\neq 2} \left(1+\frac{3}{p^s}\right), \tag{8.2}$$

where

$$S(s) = \frac{1}{2^{3s-2}} \sum_{\mathfrak{c}|2\mathbb{Z}_k} \mathcal{N}\mathfrak{c}^{s-1} z_k(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \left(1-\frac{1}{\mathcal{N}\mathfrak{p}^s}\right) T_{\mathfrak{c},2}(s),$$

for suitable $T_{\mathfrak{c},2}(s)$ detailed below and $z_k(\mathfrak{c})$ as in Definition 3.1.

We distinguish all the possible splitting types of 2 in k as above.

(1) $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_2$ of degree 2. Here $T_{\mathfrak{c},2}(s) = 1 + 1/2^s$ if $\mathfrak{c} = \mathbb{Z}_k$ or $\mathfrak{c} = \mathfrak{p}_1$, and $T_{\mathfrak{c},2}(s) = 1$ otherwise. Thus,

$$S(s) = (1/2^{3s-2})\big(1 + 1/2^s + 2^{s-1}(1-1/2^s)(1+1/2^s) + 2^{2s-2}(1-1/2^{2s}\big) + 2^{3s-2}(1-1/2^s)(1-1/2^{2s})) = 1 + 1/2^{2s} + 4/2^{3s} + 2/2^{4s}.$$

The remaining computations of $S(s)$ are exactly similar and so we omit the details.

(2) $2\mathbb{Z}_k$ is inert. Then $T_{\mathfrak{c},2}(s) = 1$ for all $\mathfrak{c}$.

(3) $2 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Then $T_{\mathfrak{c},2}(s) = 1 + 1/2^s$ if $\mathfrak{c} = \mathbb{Z}_k$ or $\mathfrak{c} = \mathfrak{p}_1$, and $T_{\mathfrak{c},2}(s) = 1$ otherwise.

(4) $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$. Here $T_{\mathfrak{c},2}(s) = 1 + 1/2^s$ for $\mathfrak{c} = \mathbb{Z}_k$ and 1 otherwise. The two different values of $S(s)$ for $\mathrm{Disc}(k) \equiv 0$ or $4 \pmod 8$ come from the different values of $z_k(\mathfrak{c})$.

(5) $2\mathbb{Z}_k = \mathfrak{p}_1^3$, i.e., 2 totally ramified. Here $T_{\mathfrak{c},2}(s) = 1$ for all $\mathfrak{c}$.

In all cases we compute that $S(s) = M_1(s)$ as given in Theorem 1.4, so that (8.2) is equal to the first term of $\Phi_k(s)$, with equality if and only if k is totally real and $2 \nmid h_2^+(k)$.

8.2 Interpreting the nontrivial characters in terms of class groups

Unless k is totally real and $2 \nmid h_2^+(k)$, Propositions 4.1 and 6.4 imply that there are also nontrivial characters.

We discuss the case $\mathfrak{c} = 1$ first. Proposition 4.1 gives an isomorphism $\phi : \mathrm{Cl}(k)/\mathrm{Cl}(k)^2 \to C_{(1)}$, and we may write a character χ of $C_{(1)}$ as a character χ_ϕ of $\mathrm{Cl}(k)/\mathrm{Cl}(k)^2$, where $\chi_\phi(\mathfrak{a}) = \chi(\phi(\mathfrak{a}))$, so that $\chi(\mathfrak{b}) = \chi_\phi(\phi^{-1}(\mathfrak{b})) = \chi_\phi(\mathfrak{b}/\sqrt{\mathcal{N}(\mathfrak{b})})$. We further use the Artin map of class field theory to rewrite χ_ϕ as a character of the quadratic field determined by $\mathrm{Ker}(\chi_\phi)$, so that $\chi_\phi(\mathfrak{p}) = 1$ if $\mathfrak{p}$ splits in this quadratic field, and $\chi_\phi(\mathfrak{p}) = -1$ if $\mathfrak{p}$ is inert.

The set of these characters corresponds precisely to the set of unramified quadratic extensions of k, i.e., fields in $\mathcal{L}(k,1)$. By Theorem 2.2 there are $a(k)$ characters for each field in $\mathcal{L}(k,1)$, where $a(k)$ is equal to 3 or 1 in the A_4 and S_4 cases respectively.

In the A_4 case, or if otherwise $C_{(1)} \simeq C_{(4)}$, Propositions 4.1 and 6.3 imply that the natural surjection $C_{\mathfrak{c}^2} \to C_1$ is an isomorphism for each $\mathfrak{c}$, and so may we regard each character χ of $C_{\mathfrak{c}^2}$ first as a character of $C_{(1)}$, and then as a character of a quadratic field as above, provided that we still write $\chi(\mathfrak{a}) = 0$ if $\mathfrak{a}$ is not coprime to $\mathfrak{c}$.

If $C_{(1)} \not\simeq C_{(4)}$, then each $C_{\mathfrak{c}^2}$ will be naturally isomorphic to either $C_{(1)}$ or $C_{(4)}$, and in Proposition 8.1 we determine which on a case-by-case basis. Those $C_{\mathfrak{c}^2}$ isomorphic to $C_{(1)}$ are handled as before. Those $C_{\mathfrak{c}^2}$ isomorphic to $C_{(4)}$ may be handled similarly: composing this isomorphism with ϕ we obtain an isomorphism with $\mathrm{Cl}_{(4)}(k)/\mathrm{Cl}_{(4)}(k)^2$, and we obtain a character associated to a quadratic field in $\mathcal{L}_2(k)$, with $\chi(\mathfrak{a}) = \chi_\phi(\mathfrak{a}/\sqrt{\mathcal{N}(\mathfrak{a})})$, except when $(\mathfrak{a},\mathfrak{c}) \neq 1$ in which case we have $\chi(\mathfrak{a}) = 0$.

This latter construction does not allow us to compute $\chi(\mathfrak{a})$ when $\mathfrak{a}$ is coprime to $\mathfrak{c}$ but not (2), and we will need to do this in two cases where $C_{\mathfrak{c}^2} \simeq C_{(4)}$. Here we apply Proposition 4.3 to extend ϕ to an isomorphism $\mathrm{Cl}_{4/\mathfrak{c}^2}(k)/\mathrm{Cl}_{4/\mathfrak{c}^2}(k)^2 \to C_{\mathfrak{c}^2}$ which agrees with the ϕ given previously on ideals coprime to (2).

Putting this all together, for each $\mathfrak{c}|(2)$ we may thus interpret the sum over nontrivial characters in $X_{\mathfrak{c}^2}$ as a sum over all quadratic extensions K_6/k, unramified at infinity, and with either $\mathfrak{d}(K_6/k) = \mathbb{Z}_k$ or $\mathfrak{d}(K_6/k)|(4)$ as appropriate. By Corollary 6.2 these correspond to quartic fields in $\mathcal{L}(k,1)$ or $\mathcal{L}_2(k)$ respectively.

8.3 Evaluating the contribution of the nontrivial characters.

We begin with the contributions of fields $L \in \mathcal{L}(k,1)$, which correspond to characters of all the groups $C_{\mathfrak{c}^2}$ occurring in Theorem 3.2.

For each $L \in \mathcal{L}(k,1)$, the contribution of the nontrivial characters is

$$\frac{S'(s)}{2^{r_2(k)}} \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2,\, p\neq 2} \left(1 + \frac{\chi_\phi(\mathfrak{p}_1)}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2,\, p\neq 2} \left(1 + \frac{\chi_\phi(\mathfrak{p}_1)}{p^s}\right) \times \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\, p\neq 2} \left(1 + \frac{\chi_\phi(\mathfrak{p}_3) + \chi_\phi(\mathfrak{p}_2) + \chi_\phi(\mathfrak{p}_1)}{p^s}\right), \quad (8.3)$$

where $S'(s)$ is a sum over the ideals dividing $2\mathbb{Z}_k$ as before, and $\chi_\phi(\mathfrak{p})$ is 1 or -1 depending on whether $\mathfrak{p}$ splits or is inert in the quadratic extension K_6/k corresponding to L.

For the three splitting types of p in k occurring in (8.3), Theorem 5.1 gives the following possible splitting types of p in K_6 and L:

- (21) in k, (42) in K_6, (4) in L. Then $\chi_\phi(\mathfrak{p}_1) = -1$.
- (21) in k, (2211) in K_6, (211) in L. Then $\chi_\phi(\mathfrak{p}_1) = 1$.
- (111) in k, (2211) in K_6, (22) in L. Then $\chi_\phi(\mathfrak{p}_3) + \chi_\phi(\mathfrak{p}_2) + \chi_\phi(\mathfrak{p}_1) = -1$.
- (111) in k, (111111) in K_6, (1111) in L. Then $\chi_\phi(\mathfrak{p}_3) + \chi_\phi(\mathfrak{p}_2) + \chi_\phi(\mathfrak{p}_1) = 3$.

- (1^21) in k, (2^211) in K_6, (21^2) in L. Then $\chi_\phi(\mathfrak{p}_1) = -1$.
- (1^21) in k, (1^21^211) in K_6, (1^211) in L. Then $\chi_\phi(\mathfrak{p}_1) = 1$.

These match the values of $\omega_L(p)$ given in Definition 1.3, as required.

Once again we have

$$S'(s) = \frac{1}{2^{3s-2}} \sum_{\mathfrak{c}} \mathcal{N}\mathfrak{c}^{s-1} z_k(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^s}\right) T_{\mathfrak{c},2}(s) \,, \tag{8.4}$$

where $\mathfrak{c}$ ranges over all ideals dividing $2\mathbb{Z}_k$, and $T_{\mathfrak{c},2}(s)$ now depends on the splitting of 2 in K_6. For example, if 2 is totally split in $\mathbb{Z}_k$ as $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ and K_6/k is unramified, we check that $T_{\mathfrak{c},2}(s)$ is equal to $1 + \omega_L(2)/2^s$ for $\mathfrak{c} = \mathbb{Z}_k$, and $1 \pm \frac{1}{2^s}$ for $\mathfrak{c} = \mathfrak{p}_i$, depending on whether $\mathfrak{p}_i$ is split or inert in K_6/k. The proof that $S'(s) = M_{2,L}(s)$ breaks up into six cases depending on the splitting type of 2 in k, and, when 2 is partially ramified, $\mathrm{Disc}(k) \pmod 8$. The computation is similar to our previous computations and we omit the details. Applying this computation with the $n^2 = 1$ entries of Proposition 7.1 and the values of $\chi_\phi(\mathfrak{p}_i)$ just computed, we obtain the $n^2 = 1$ entries in the table of Theorem 1.4.

Recall from Propositions 4.1 and 6.4 that either $|C_4| = |C_1|$ or $|C_{(4)}| = 2|C_{(1)}|$, hence either $|\mathcal{L}_2(k)| = |\mathcal{L}(k,1)|$ or $2|\mathcal{L}(k,1)| + 1$. If $|\mathcal{L}_2(k)| = |\mathcal{L}(k,1)|$, and in particular in the A_4 case, the proof of Theorem 1.4 is now complete.

8.4 The case where $|\mathcal{L}_2(k)| = 2|\mathcal{L}(k,1)| + 1$

We henceforth assume that $|\mathcal{L}_2(k)| = 2|\mathcal{L}(k,1)| + 1$, in which case we must also compute the contributions from the fields in $\mathcal{L}_2(k)\backslash\mathcal{L}(k,1)$. $F_k(\chi, s)$ is evaluated in essentially the same way, but in (8.4) we sum over only those $\mathfrak{c}$ for which $|C_{\mathfrak{c}^2}| = |C_{(4)}|$. To compute $S'(s)$ we must therefore compute a list of such $\mathfrak{c}'$.

Proposition 8.1. *Assume that* $|C_{(4)}| = 2|C_{(1)}|$ *and* $|\mathcal{L}_2(k)| = 2|\mathcal{L}(k,1)| + 1$, *so that exactly one of* $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, *or* $\mathcal{L}_{tr}(k,64)$ *is nonempty. Then, for* $\mathfrak{c}|(2)$, $|C_{\mathfrak{c}^2}| = 2|C_{(1)}|$ *if and only if* $\mathfrak{c}$ *is one of the following ideals:*

If $\mathcal{L}(k,4)$ *is nonempty:*

- *If* 2 *is* $(1^21)_0$, $\mathfrak{c} = \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_1^2, \mathfrak{p}_1\mathfrak{p}_2, (2)$.
- *If* 2 *is* $(1^21)_4$, $\mathfrak{c} = \mathfrak{p}_1, \mathfrak{p}_1^2, \mathfrak{p}_1\mathfrak{p}_2, (2)$.
- *If* 2 *is* (1^3), $\mathfrak{c} = \mathfrak{p}, \mathfrak{p}^2, (2)$.

If $\mathcal{L}(k,16)$ *is nonempty:*

- *If* 2 *is* (21), $\mathfrak{c} = \mathfrak{p}_1, \mathfrak{p}_2, (2)$.
- *If* 2 *is* (111), $\mathfrak{c} = \mathfrak{p}_1, \mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_3, \mathfrak{p}_2\mathfrak{p}_3, (2)$. *The distinguished prime ideal* $\mathfrak{p}_1$ *is the prime ideal not ramified in* K_6/k *for* K_6 *corresponding to* $\mathcal{L}(k,16)$.
- *If* 2 *is* (1^21) (*necessarily* $(1^21)_4$), $\mathfrak{c} = \mathfrak{p}_1^2, (2)$.

If $\mathcal{L}_{tr}(k,64)$ *is nonempty:*

- *If* 2 *is* (3), $\mathfrak{c} = (2)$.
- *If* 2 *is* (21), $\mathfrak{c} = \mathfrak{p}_2, (2)$.
- *If* 2 *is* (1^21) (*necessarily* $(1^21)_0$), $\mathfrak{c} = \mathfrak{p}_1^2, (2)$.
- *If* 2 *is* (1^3), $\mathfrak{c} = (2)$.

Proof. First observe from (3) of Proposition 4.1 that if some $\mathfrak{c}$ appears on the list, so do all of its multiples, and conversely if some $\mathfrak{c}$ does not, neither do its factors.

As the size of $C_{\mathfrak{c}^2} = \mathrm{Cl}^S_{\mathfrak{c}^2}(f)/D^S_{\mathfrak{c}^2}$ is measured by the exact sequence of Proposition 3.13, we consider the change in the size of the other factors when we replace $\mathfrak{c}$ by a multiple $\mathfrak{c}'$ of $\mathfrak{c}$. Two other factors may change in (3.2):

- The quantity $Z^S_{\mathfrak{c}}/Z^2_{\mathfrak{c}}$ may increase in size; this is necessary but not sufficient for $C_{\mathfrak{c}^2}$ to increase in size. By Proposition 3.15, $|Z^S_{\mathfrak{c}}/Z^2_{\mathfrak{c}}| = \mathcal{N}(\mathfrak{c})/z_k(\mathfrak{c})$ where $z_k(\mathfrak{c})$ is defined in Definition 3.1 (see also Theorem 3.20).
- The quantity $S^S_{\mathfrak{c}^2}$ may decrease in size. Then $Z^S_{\mathfrak{c}}/Z^2_{\mathfrak{c}}$ must increase, and by a larger proportion if $|C_{\mathfrak{c}^2}|$ also increases.
  To check this possibility, observe that Proposition 3.3 implies that the equality $S^S_{\mathfrak{c}^2} = S^S_{\mathfrak{c}'^2}$ with $\mathfrak{c}|\mathfrak{c}'$ is equivalent to the fact that all quadratic extensions of k, corresponding to fields in $\mathcal{L}^*_2(k)$ (that is, $\mathcal{L}_2(k)$ without the signature restriction), whose discriminants divide $4/\mathfrak{c}^2$ must in fact have discriminants dividing $4/\mathfrak{c}'^2$.

This information is enough to prove the proposition; we explain in detail for a representative case, and give a sketch for the remaining cases.

Suppose that $(2) = \mathfrak{p}_1^2\mathfrak{p}_2$ in L with $d = \mathrm{Disc}(k) \equiv 0 \pmod 8$. By Definition 3.1, $z_k(\mathfrak{c})$ doubles when $\mathfrak{c}$ increases from $\mathfrak{p}_1^2$ to (2), or from $\mathfrak{p}_1$ or $\mathfrak{p}_2$ to $\mathfrak{p}_1\mathfrak{p}_2$. $\mathcal{N}(\mathfrak{c})$ also doubles in each of these cases and so $|C_{\mathfrak{c}^2}|$ stays the same.

There are quartic fields of discriminant $4d$ or $64d$, but not both. In the former case, $|S^S_{\mathfrak{c}^2}|$ decreases when $\mathfrak{c}$ goes to (2) from either $\mathfrak{p}_1\mathfrak{p}_2$ or $\mathfrak{p}_1^2$, or both. We can rule out $\mathfrak{p}_1^2$, because $\mathcal{N}(\mathfrak{p}_1^2)/z_k(\mathfrak{p}_1^2) = \mathcal{N}(2)/z_k((2))$. Therefore $|S^S_{(\mathfrak{p}_1\mathfrak{p}_2)^2}(k)| = 2|S^S_{(4)}(k)|$, and so $|C_{(\mathfrak{p}_1\mathfrak{p}_2)^2}| = |C_{(4)}|$. Put together, these observations establish that $|C_{\mathfrak{c}^2}|$ is the same for all $\mathfrak{c} \in \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_1^2, \mathfrak{p}_1\mathfrak{p}_2, (2)\}$, as claimed.[8]

If instead there are quartic fields of discriminant $64d$, then $|S^S_{\mathfrak{c}^2}|$ decreases when $\mathfrak{c}$ goes from 1 to either $\mathfrak{p}_1$ or $\mathfrak{p}_2$. As $\mathcal{N}(\mathfrak{c})/z_k(\mathfrak{c})$ doubles, $|C_{\mathfrak{c}^2}|$ stays the same. Therefore, $|C_{\mathfrak{c}^2}|$ is the same for $\mathfrak{c} \in \{\mathfrak{p}_1^2, (2)\}$, and separately for all $\mathfrak{c} \in \{1, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_2\}$, proving this case of the proposition.

The remaining cases are similar, and we omit the details. Some brief remarks, helpful for verifying the results:

- When 2 is (1^21) in k the values of $z_k(\mathfrak{c})$ depend on whether $\mathrm{Disc}(k)$ is 0 or 4 (mod 8), explaining the different results for these two cases.
- When 2 is (21) in k and $\mathcal{L}_{tr}(k, 64) \neq \emptyset$, $|S^S_{\mathfrak{c}^2}(k)|$ decreases when $\mathfrak{c}$ increases from $\mathbb{Z}_k$ to $\mathfrak{p}_2$, but $|\mathcal{N}(\mathfrak{c})/z_k(\mathfrak{c})|$ increases by a factor of 4 and we cannot conclude that $|C_{\mathfrak{c}^2}|$ remains the same. Indeed, $\mathcal{N}(\mathfrak{p}_2)/z_k(\mathfrak{p}_2) = \mathcal{N}(2)/z_k((2))$, and $2\mathcal{N}(1)/z_k((1)) = \mathcal{N}(\mathfrak{p}_1)/z_k(\mathfrak{p}_1)$ with a decrease in $|S^S_{\mathfrak{c}^2}(k)|$, so that $|C_{\mathfrak{p}_2^2}| = |C_{(4)}|$ and $|C_{(1)}| = |C_{\mathfrak{p}_1^2}|$, so that by elimination we deduce that $|C_{\mathfrak{p}_1^2}| \neq |C_{(4)}|$.
- When 2 is (111), $\mathcal{L}(k, 16)$ is nonempty, and the corresponding extensions K_6/k must all have the same discriminant, corresponding to an increase of 1 in the 2-rank of appropriate ray class groups. This discriminant is $(\mathfrak{p}\mathfrak{p}')^2$ for two of the primes $\mathfrak{p}$, $\mathfrak{p}'$ of k above 2, and we write $\mathfrak{p}_1$ for the remaining prime.

□

[8] Moreover, observe that this tells us that the associated quadratic extensions $K_6 = k(\sqrt{\alpha})$ satisfy $\mathfrak{d}(K_6/k) = \mathfrak{p}_1^2$. This adds information to what we determined in the proof of Proposition 7.3; conversely, in cases where we determined this information in Proposition 7.3, we could apply it in the present proof (although in each case it can be determined from the statement of Proposition 7.3 and the considerations described above).

Remark. Recall that this statement was applied in the proof of Proposition 4.3. In that proof, that the size of jClc02(k) = Clc02(k)2j is as claimed may be deduced from the conditions on the L(k; n2), from class eld theory, and from the discriminant relation in Theorem 2.2.

For each L in $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, and $\mathcal{L}_{tr}(k,64)$, we can now prove that $S'(s) = M_{2,L}(s)$. The analysis again breaks up into cases, and we present the details for a representative case.

Suppose then that $L \in \mathcal{L}(k,16)$ and that 2 is totally split in L. As before write $\mathfrak{p}_1$ for the prime of k above 2 which does not ramify in the extension K_6/k corresponding to L, and write $\mathfrak{p}_2$, $\mathfrak{p}_3$ for the other two primes above 2. By Theorem 3.2 we have

$$T_{\mathfrak{c},2}(s) = \frac{1 + \chi(\mathfrak{p}_1\mathfrak{p}_2) + \chi(\mathfrak{p}_1\mathfrak{p}_3) + \chi(\mathfrak{p}_2\mathfrak{p}_3)}{2^s}, \tag{8.5}$$

where for each $\mathfrak{c}$, $\chi(\mathfrak{p}_i\mathfrak{p}_j) = \chi_\phi(2/\mathfrak{p}_i\mathfrak{p}_j)$ if $\mathfrak{p}_i\mathfrak{p}_j$ is coprime to $\mathfrak{c}$, and $\chi(\mathfrak{p}_i\mathfrak{p}_j) = 0$ otherwise. In particular, we have $T_{\mathfrak{c},2}(s) = 1 + \frac{\chi_\phi(\mathfrak{p}_1)}{2^s}$ when $\mathfrak{c} = \mathfrak{p}_1$, and $T_{\mathfrak{c},2}(s) = 1$ for the other $\mathfrak{c}$ listed in Proposition 8.1. By Proposition 8.1 we obtain contributions to $S'(s)$ from the ideals $\mathfrak{c} = \mathfrak{p}_1, \mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_3, \mathfrak{p}_2\mathfrak{p}_3, (2)$ as follows:

- $\mathfrak{c} = \mathfrak{p}_1$: $\frac{4}{8^s} \cdot \frac{2^s}{2} \cdot \left(1 - \frac{1}{2^s}\right)\left(1 + \frac{\chi_\phi(\mathfrak{p}_1)}{2^s}\right) = 2 \cdot 2^{-2s} + 2(\chi_\phi(\mathfrak{p}_1) - 1)2^{-3s} - 2\chi_\phi(\mathfrak{p}_1)2^{-4s}$.
- $\mathfrak{c} = \mathfrak{p}\mathfrak{p}'$: $\frac{4}{8^s} \cdot \frac{4^s}{4} \cdot \left(1 - \frac{1}{2^s}\right)^2 = 2^{-s} - 2 \cdot 2^{-2s} + 2^{-3s}$.
- $\mathfrak{c} = (2)$: $\frac{4}{8^s} \cdot \frac{8^s}{4} \cdot \left(1 - \frac{1}{2^s}\right)^3 = 1 - 3 \cdot 2^{-s} + 3 \cdot 2^{-2s} - 2^{-3s}$.

Adding each of these contributions (with three ideals of the form $\mathfrak{p}\mathfrak{p}'$), we obtain a total of $1 - 2^{-2s} + 2\chi_\phi(\mathfrak{p})2^{-3s} - 2\chi_\phi(\mathfrak{p})2^{-4s}$. If $L \in \mathcal{L}(k,16)$, then $\mathfrak{d}(K_6/k) = (\mathfrak{p}_2\mathfrak{p}_3)^2$ and $\mathfrak{p}_1$ can split or be inert in K_6. If it splits, then $\chi_\phi(\mathfrak{p}) = 1$, and Theorem 5.1 implies that the splitting type of 2 in L is $(1^2 1^2)$, and the above contribution is $1 - 2^{-2s} + 2 \cdot 2^{-3s} - 2 \cdot 2^{-4s}$; if it is inert, then Theorem 5.1 implies that the splitting type of 2 in L is (2^2), and the above contribution is $1 - 2^{-2s} - 2 \cdot 2^{-3s} + 2 \cdot 2^{-4s}$.

This verifies that $S'(s) = M_{2,L}(s)$ for this case, and the remaining cases are proved in the same way. The only remaining case where $\mathfrak{c} \neq 1$ is $T_{\mathfrak{c},2}(s) = 1 + \chi_\phi(\mathfrak{p}_1)/2^s$ when $L \in \mathcal{L}(k,16)$, 2 is partially split, and $\mathfrak{c} = \mathfrak{p}_1$, where once again $C_{\mathfrak{c}^2} \simeq \mathrm{Cl}_{4/\mathfrak{c}^2}/\mathrm{Cl}^2_{4/\mathfrak{c}^2}$. In the other cases $T_{\mathfrak{c},2}(s) = 1$ and the computations are simpler; in particular, it suffices to appeal to Proposition 4.1 rather than Proposition 4.3.

For each combination of possibilities for n^2 and the splitting types of K_6 and L listed in Proposition 7.1, we thus check that $S'(s) = M_{2,L}(s)$, and the product over primes $p \neq 2$ is handled as in (8.3). This completes the proof.

9 Results with signatures

In the case of cubic fields with given quadratic resolvent, the quadratic resolvent determines the signature of the cubic field. In our case this is not true: if k is a complex cubic field then the corresponding quartic fields K have signature $(2,1)$, but if k is a totally real cubic then K can either be totally real (signature $(4,0)$), or totally complex (signature $(0,2)$), and we may want to separate these families.

As mentioned in [7] and [12], it is possible to modify the above work to take into account signature constraints (or more generally a finite number of local conditions). Since there are no new results when k is complex, in this section we always assume that k is a totally real cubic field.

We define $\mathcal{F}^+(k)$ as the subset of all totally real quartic fields in $\mathcal{F}(k)$, and define

$$\Phi_k^+(s) = \frac{1}{a(k)} + \sum_{K \in \mathcal{F}^+(k)} \frac{1}{f(K)^s} .$$

We define $\mathcal{L}_2^*(k)$ and $\mathcal{L}^*(k,1)$ as in Definition 1.2, only without any restriction that the quartics be totally real. In this setting we have the following:

Theorem 9.1. *The formulas of Theorem 1.4 hold for $\Phi_k^+(s)$ with the following two modifications:*

- *The formulas are multiplied by $\frac{1}{4}$.*
- *The sums over $\mathcal{L}_2(k)$ and $\mathcal{L}(k,1)$ are replaced with sums over $\mathcal{L}_2^*(k)$ and $\mathcal{L}^*(k,1)$.*

This result exhibits a curious duality: in order to enumerate quartic fields *with* signature conditions, we sum over fields in $\mathcal{L}_2^*(k)$ *without* signature conditions.

9.1 Theorem 3.2 with signature conditions

We first sketch a proof of a version of Theorem 3.2 for this setting, mainly explaining the difference with the case where no signature conditions are added.

Theorem 9.2.

$$\Phi_k^+(s) = \frac{1}{a(k)2^{3s}} \sum_{\mathfrak{c} | 2\mathbb{Z}_k} \mathcal{N}\mathfrak{c}^{s-1} z_k(\mathfrak{c}) \prod_{\mathfrak{p} | \mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^s}\right) \sum_{\chi \in X_{\mathfrak{c}^2}^+} F_k(\chi, s) ,$$

where $X_{\mathfrak{c}^2}^+$ is the group of characters of $C_{\mathfrak{c}^2}^+$, defined as $C_{\mathfrak{c}^2}$ with the added condition that β be totally positive, and $z_k(\mathfrak{c})$ and $F_k(\chi, s)$ are as in Theorem 3.2.

Proof. The condition that K is totally real is equivalent to the fact that the corresponding quadratic extension of trivial norm K_6/k is unramified at infinity, or equivalently that $K_6 = k(\sqrt{\alpha})$ with α totally positive. In Proposition 3.7 we must replace the condition $\overline{u} \in S^S(k)$ by $\overline{u} \in S^+(k)$ and require $\mathfrak{a}$ to represent a square in $\mathrm{Cl}^+(k)$, and in the beginning of the computation of $\Phi_k(s)$ after that proposition we must similarly replace all occurrences of $S^S(k)$ by $S^+(k)$.

In definitions 3.1 and 3.10 we must add superscripts $^+$ to all the groups which are defined, adding everywhere the condition that β or u is totally positive (in the language of class field theory, we write $\beta \equiv 1 \pmod{{}^*\mathfrak{c}^2 S_\infty}$, where S_∞ is the modulus made of the three infinite places of k). We write $Z_{\mathfrak{c}}^+$ for the set of elements of $(\mathbb{Z}_k/\mathfrak{c}^2)^*$ which have a totally positive lift, but it is easily checked that $Z_{\mathfrak{c}}^+ = Z_{\mathfrak{c}}$ and $Z_{\mathfrak{c}}^{+,S} = Z_{\mathfrak{c}}^S$, and hence that $z_k^+(\mathfrak{c}) = z_k(\mathfrak{c})$, so we do not need to compute again this subtle quantity.

We also check that $S_{\mathfrak{c}^2}^{+,S} = S_{\mathfrak{c}^2}^+$, and the exact sequence corresponding to (3.2) of Proposition 3.13 is thus

$$1 \longrightarrow S_{\mathfrak{c}^2}^+(k) \longrightarrow S^+(k) \longrightarrow \frac{Z_{\mathfrak{c}}^S}{Z_{\mathfrak{c}}^2} \longrightarrow C_{\mathfrak{c}^2}^+ \longrightarrow C_{(1)}^+ \longrightarrow 1 . \tag{9.1}$$

The computations leading to Corollary 3.12 are identical, and that corollary is thus valid if we replace $\Phi_k(s)$, $S_{\mathfrak{c}^2}^S(k)$, $C_{\mathfrak{c}^2}$, $X_{\mathfrak{c}^2}$ by the corresponding values with $^+$ superscripts.

By Proposition 3.3 and Lemma 3.6, $|S^+(k)|$ and $|S^+_{(4)}(k)|$ are respectively equal to the number of quadratic extensions of k, together with the trivial extension k/k, which are unramified at infinity and whose discriminants divide (4) and (1) respectively, which implies the equalities $|S^+(k)| = |\mathrm{Cl}_{(4)}(k)/\mathrm{Cl}_{(4)}(k)^2|$ and $|S^+_{(4)}(k)| = |\mathrm{Cl}(k)/\mathrm{Cl}(k)^2|$. Note the reversal of the 4 and 1, a consequence of Hecke's discriminant computation.

It is also known ([9], Proposition 4.7) that $|\mathrm{Cl}_{(4)}(k)/\mathrm{Cl}_{(4)}(k)^2| = |\mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2|$ and hence the proof of Corollary 3.14 becomes

$$|S^+_{\mathfrak{c}^2}(k)||Z^S_{\mathfrak{c}}/Z^2_{\mathfrak{c}}||C^+_{(1)}| = |S^+(k)||C^+_{\mathfrak{c}^2}| = |\mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2||C^+_{\mathfrak{c}^2}| = |C^+_{(1)}||C^+_{\mathfrak{c}^2}|\,,$$

where we have also extended (3) of Proposition 3.13; in other words

$$|S^+_{\mathfrak{c}^2}(k)|/|C^+_{\mathfrak{c}^2}| = 1/|Z^S_{\mathfrak{c}}/Z^2_{\mathfrak{c}}| = z_k(\mathfrak{c})/\mathcal{N}(\mathfrak{c})$$

by Lemma 3.15. Putting everything together proves the theorem. □

Remark. As in Theorem 9.1, there are exactly two differences between the formula of Theorem 9.2 and that of Theorem 3.2: we sum on $\chi \in X^+_{\mathfrak{c}^2}$ instead of $\chi \in X_{\mathfrak{c}^2}$, and the factor in front of $1/(a(k)2^{3s})$ is 1 instead of $2^{2-r_2(k)} = 4$.

Since only the trivial characters contribute to asymptotics, this implies (as already mentioned in [7]) that the number of totally real quartics $L \in \mathcal{F}(k)$ and positive discriminant up to X is asymptotically 1/4 of the total number, independently of the signatures of the fundamental units. The same is also true without the specification of a cubic resolvent field, as proved by Bhargava [5].

9.2 The main theorem with signature conditions

It is readily checked that the map $\phi : \mathfrak{a} \to \mathfrak{a}/\mathcal{N}(\mathfrak{a})$ of Proposition 4.1 (1) also yields an isomorphism $\mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2 \simeq C^+_{(1)}$. It also yields a surjective homomorphism

$$\mathrm{Cl}^+_{(4)}(k)/\mathrm{Cl}^+_{(4)}(k)^2 \to C^+_{(4)} \tag{9.2}$$

which is not an isomorphism, but is rather two-to-one. Writing A for the kernel (of the map $\mathrm{Cl}^+_{(4)} \to C^+_{(4)}$), we check that A is represented by the class of (p) for any rational prime $p \equiv 3 \pmod 4$ which is inert in k.

Lemma 7.9. *The quadratic extensions k_6/k which correspond, by class field theory, to subgroups of $\mathrm{Cl}^+_{(4)}(k)/A$ of index 2 are precisely those which correspond, by Theorem 2.2, to quartic fields in $\mathcal{L}^*_2(k)$.*

Proof. Let $\mathcal{Q}$ denote the set of quadratic extensions k_6/k, including the trivial extension k/k, which have conductor dividing $4\mathbb{Z}_k$, and which by Lemma 3.6 are generated by the square root of a virtual unit. Let $\mathcal{Q}'$ denote the set of such extensions which in addition are generated by a virtual unit of square norm (in this case, of norm 1); by Theorem 2.2 these are the extensions which correspond to fields in $\mathcal{L}^*_2(k)$. Since exactly one of α or $-\alpha$ is of square norm for each virtual unit α, we have $|\mathcal{Q}'| = \frac{1}{2}|\mathcal{Q}|$.

Class field theory provides a bijection between $\mathcal{Q}$ and index 2 subgroups of $\mathrm{Cl}^+_{(4)}(k)/\mathrm{Cl}^+_{(4)}(k)^2$. Write $\mathcal{Q}''$ for the set of extensions corresponding to subgroups of $\mathrm{Cl}^+_{(4)}(k)/A$; then the fields $k_6 \in \mathcal{Q}''$ have the additional property that all rational primes $\equiv 3 \pmod 4$ which are inert in k split completely in k_6.

By (5.1), this latter property is a necessary condition for any such k_6 to be in $\mathcal{Q}'$, so that $\mathcal{Q}' \subseteq \mathcal{Q}''$. But since $|\mathcal{Q}''| = \frac{1}{2}|\mathcal{Q}|$ (as (9.2) is two-to-one) and $|\mathcal{Q}'| = \frac{1}{2}|\mathcal{Q}|$, we must therefore have $\mathcal{Q}'' = \mathcal{Q}'$, the desired conclusion. □

Remark. By the same token, for each $\mathfrak{c} \mid 2\mathbb{Z}_k$, the quadratic extensions corresponding to subgroups of $\mathrm{Cl}^+_{\mathfrak{c}^2}(k)/(A \cup \mathrm{Cl}^+_{\mathfrak{c}^2}(k)^2)$ are those which further satisfy $\mathfrak{d}(k_6/k) \mid \mathfrak{c}^2$. (By slight abuse of notation we also write A for the image of the previously defined A under the canonical surjection $\mathrm{Cl}^+_{(4)}(k) \to \mathrm{Cl}^+_{\mathfrak{c}^2}(k)$.)

The natural analogue of the first part of (3) of Proposition 4.1 also holds as well. In place of (2), we obtain the following:

Lemma 9.3. *We have the following equalities:*

$$\frac{|C^+_{(4)}|}{|C^+_{(1)}|} \cdot \frac{|C_{(4)}|}{|C_{(1)}|} = 4, \tag{9.3}$$

$$|C_{(4)}| = |C^+_{(1)}|. \tag{9.4}$$

Therefore, $|C^+_{(4)}|/|C^+_{(1)}|$ is equal to 2 or 4, depending on whether there does or does not exist a nonsquare totally positive unit.

Proof. By (9.1), we have

$$\frac{|C^+_{(4)}|}{|C^+_{(1)}|} \cdot \frac{|S^+(k)|}{|S^+_{(4)}(k)|} = 4. \tag{9.5}$$

Recall from earlier that $|S^+(k)| = |\mathrm{Cl}_{(4)}(k)/\mathrm{Cl}_{(4)}(k)^2| = |\mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2|$ and $|S^+_{(4)}(k)| = |\mathrm{Cl}(k)/\mathrm{Cl}(k)^2|$; we immediately obtain (9.4) and (9.3) from these computations and the various isomorphisms proved in Proposition 4.1 (1) and its extension. The final statement then follows from (2) of Proposition 4.1. □

The results of Section 5 apply equally to this setting. Theorem 6.1 also holds, with the same proof, where we replace $\mathcal{L}_2(k)$ with $\mathcal{L}^*_2(k)$ and $V^+(k)$ with $V^S(k)$. Analogues of (1) and the first part of (2) of Proposition 6.4 hold, with $\mathcal{L}(k,1)$, $\mathcal{L}_2(k)$, $\mathrm{rk}_2(k)$, $C_{(n)}$ replaced with $\mathcal{L}^*(k,1)$, $\mathcal{L}^*_2(k)$, $\mathrm{rk}^+_2(k)$, $C^+_{(n)}$ respectively. However, in light of Lemma 9.3 the remainder of Proposition 6.4 no longer holds, and in particular it is not true that at most one of $\mathcal{L}(k,4)$, $\mathcal{L}(k,16)$, and $\mathcal{L}_{tr}(k,64)$ can be nonempty.

Results analogous to those of Section 7 hold, with the same proofs, except that in Proposition 7.3 and the first part of Remarks 7.4, the conditions on the valuations of $\alpha \in W^+(k)$ appearing in the various cases are no longer mutually exclusive.

Finally, it is reasonably straightforward to adapt the arguments of Section 8. The key step is that we require, for each $\mathfrak{c}|(2)$, an isomorphism

$$\mathrm{Cl}^+_{\mathfrak{c}'^2}(k)/(A \cup \mathrm{Cl}^+_{\mathfrak{c}'^2}(k)^2) \xrightarrow{\phi} C^+_{\mathfrak{c}^2} \tag{8.6}$$

for appropriate $\mathfrak{c}'|(2)$, which satisfies $\phi(\mathfrak{a}) = \mathfrak{a}/\mathcal{N}(\mathfrak{a})$ for $\mathfrak{a}$ coprime to 2, and also for $\mathfrak{a}$ not coprime to 2 in the two cases of Proposition 4.3. We already observed that the proof of Proposition 4.1 yields such an isomorphism for $\mathfrak{c} = \mathfrak{c}' = (2)$ and $\mathfrak{c} = \mathfrak{c}' = (1)$, and the

proof of Proposition 4.3 also gives such an isomorphism in the special cases described there.

If $|C^+_{(4)}| = 2|C^+_{(1)}|$ then, as before, each $C^+_{\mathfrak{c}^2}$ is canonically isomorphic to either $C^+_{(1)}$ or $C^+_{(4)}$, giving an isomorphism (8.6) for each $\mathfrak{c}$, and the proof of the proposition goes through without essential change. In the second bullet point in the proof of Proposition 8.1, the equality $S^+_{\mathfrak{c}^2} = S^+_{\mathfrak{c}'^2}$ implies the stated condition only for fields in $\mathcal{L}_2(k)$, insufficient to imply what follows. However in this case we must have $\frac{|C^+_{\mathfrak{c}^2}|}{|C^+_{(1)}|} = \frac{|C_{\mathfrak{c}^2}|}{|C_{(1)}|}$ for each $\mathfrak{c} \mid 2\mathbb{Z}_k$: this follows because of the implications $|C_{\mathfrak{c}^2}| = |C_{(1)}| \implies |C^+_{\mathfrak{c}^2}| = |C^+_{(1)}|$ and $|C_{\mathfrak{c}^2}| = |C_{(4)}| \implies |C^+_{\mathfrak{c}^2}| = |C^+_{(4)}|$, which follow from the definitions of the $C_{\mathfrak{c}^2}$. In particular, the stated condition discussed earlier also applies with respect to $\mathcal{L}^*_2(k)$, as needed for the remainder of the proof.

If instead $|C^+_{(4)}| = 4|C^+_{(1)}|$ we have $S^+(k) = S^+_{\mathfrak{c}^2}(k)$ for each $\mathfrak{c}$ and thus $|C^+_{\mathfrak{c}^2}| = \frac{\mathcal{N}(\mathfrak{c})}{z_k(\mathfrak{c})}|C^+_{(1)}|$ by (9.1). When $|C^+_{\mathfrak{c}^2}|$ equals $|C^+_{(1)}|$ or $|C^+_{(4)}|$, then the associated fields in $\mathcal{L}^*_2(k)$ are respectively those in $\mathcal{L}^*(k,1)$ or (all of) $\mathcal{L}^*_2(k)$.

It remains to consider the $\mathfrak{c}$ with $|C^+_{\mathfrak{c}^2}| = 2|C^+_{(1)}|$. We have a canonical isomorphism $C^+_{\widetilde{\mathfrak{c}}^2} \simeq C^+_{\mathfrak{c}^2}$ whenever $\widetilde{\mathfrak{c}} \mid \mathfrak{c}$ or $\mathfrak{c} \mid \widetilde{\mathfrak{c}}$ and $|C^+_{\widetilde{\mathfrak{c}}^2}| = |C^+_{\mathfrak{c}^2}|$, and we will see that this reduces us to considering the following four cases: $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$ and $\mathfrak{c} = \mathfrak{p}_1$; $2\mathbb{Z}_k = \mathfrak{p}_1^3$ and $\mathfrak{c} = \mathfrak{p}_1$; $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ with each $\mathfrak{p}_i$ of inertial degree i and $\mathfrak{c} = \mathfrak{p}_1$; $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{c} = \mathfrak{p}_1$. In each case, the proof of Proposition 4.3 yields an isomorphism

$$\mathrm{Cl}^+_{(4)/\mathfrak{c}^2}(k)/(A \cup \mathrm{Cl}^+_{(4)/\mathfrak{c}^2}(k)^2) \to C^+_{\mathfrak{c}^2}\,, \tag{8.7}$$

provided that both sides of (8.7) have the same size; indeed, we have

$$\frac{|\mathrm{Cl}^+_{(4)/\mathfrak{c}^2}(k)/(A \cup \mathrm{Cl}^+_{(4)/\mathfrak{c}^2}(k)^2)|}{|\mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2|} = \frac{|S^S(k)|}{|S^S_{\mathfrak{c}^2}(k)|} = \frac{\mathcal{N}(\mathfrak{c})}{z_k(\mathfrak{c})} = 2\,,$$

by: Proposition 3.3, Lemma 3.6, Lemma 7.9 and the subsequent remark; (9.3) and (3.2); and our computation of $z_k(\mathfrak{c})$. Since $|\mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2| = |C^+_{(1)}|$, (8.7) is indeed an isomorphism of the desired shape.

The result of Proposition 8.1 still describes the set of $\mathfrak{c}$ associated to each field in $\mathcal{L}^*_2(k)$. For the splitting types $(1^2 1)$, (1^3), and (21), two of $\mathcal{L}^*(k,4)$, $\mathcal{L}^*(k,16)$, and $\mathcal{L}^*_{tr}(k,64)$ are nonempty, as we previously observed was possible in Proposition 7.3, and the proposition may be interpreted as saying that $|C^+_{\mathfrak{c}^2}| = 2|C^+_{(1)}|$ for $\mathfrak{c}$ appearing for one of them, and $|C^+_{\mathfrak{c}^2}| = 4|C^+_{(1)}|$ for $\mathfrak{c}$ appearing for both of them.

When 2 is (111), then only $\mathcal{L}^*(k,16)$ is nonempty, but all three primes $\mathfrak{p}_i$ are 'distinguished' for different fields in $\mathcal{L}(k,16)$; we have $|C^+_{\mathfrak{c}^2}| = 2|C^+_{(1)}|$ when $\mathfrak{c}$ is prime, and $|C^+_{(4)}| = 4|C^+_{(1)}|$ when $\mathfrak{c}$ is a product of two or all three primes.

From this, the conclusion of the proof of the main theorem is the same, including all of our computations of $M_{2,L}$, so that Theorem 9.1 follows from Theorem 9.2 in the same way that Theorem 1.4 followed from Theorem 3.2.

Some explicit numerical examples are worked out in Section 10.

10 Numerical computations

We finish the paper by presenting some numerical examples in a few cases representative of our main results. The proofs are immediate; the explicit number fields described below may be looked up in databases such as [22,26].

10.1 Examples for the A_4-quartic case

- $\mathrm{rk}_2(k) = 0$ **and** 2 **inert in** k:

  k cyclic cubic of discriminant $49 = 7^2$, defined by $x^3 - x^2 - 2x + 1 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{3}{p^s}\right) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p \equiv \pm 1 \pmod 7} \left(1 + \frac{3}{p^s}\right).$$

  The second equality comes from the fact that we are in an abelian situation, so such equalities also exist in the subsequent formulas.

- $\mathrm{rk}_2(k) = 2$ **and** 2 **inert in** k:

  k cyclic cubic of discriminant $26569 = 163^2$, defined by $x^3 - x^2 - 54x + 169 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{3}{p^s}\right) + \left(1 + \frac{3}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\omega_L(p)}{p^s}\right),$$

  where L is the unique A_4-quartic field with cubic resolvent k, defined by $x^4 - x^3 - 7x^2 + 2x + 9 = 0$.

- $\mathrm{rk}_2(k) = 4$ **and** 2 **totally split in** k:

  k cyclic cubic of discriminant $1019077929 = 31923^2$, defined by $x^3 - 10641x - 227008 = 0$.

$$\begin{aligned}\Phi_k(s) = {} & \frac{1}{3}\left(1 + \frac{3}{2^{2s}} + \frac{6}{2^{3s}} + \frac{6}{2^{4s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1 + \frac{3}{p^s}\right) \\ & + \left(1 + \frac{3}{2^{2s}} + \frac{6}{2^{3s}} + \frac{6}{2^{4s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1 + \frac{\omega_{L_1}(p)}{p^s}\right) \\ & + \left(1 + \frac{3}{2^{2s}} - \frac{2}{2^{3s}} - \frac{2}{2^{4s}}\right) \sum_{2\le i\le 5} \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1 + \frac{\omega_{L_i}(p)}{p^s}\right),\end{aligned}$$

  where the L_i are the five A_4-quartic fields with cubic resolvent k, defined by the respective equations $x^4 - 2x^3 - 279x^2 - 1276x + 2132$, $x^4 - 2x^3 - 207x^2 - 108x + 4464$, $x^4 - 2x^3 - 201x^2 + 154x + 4537$, $x^4 - 2x^3 - 255x^2 - 40x + 13223$, $x^4 - x^3 - 237x^2 + 132x + 13908$, and L_1 is distinguished by being the only one of the five fields in which 2 is totally split.

10.2 Examples for the S_4-quartic case

- k defined by $x^3 - x^2 - 3x + 1 = 0$, $\mathrm{Disc}(k) = 148$, $\mathrm{rk}_2^+(k) = 0$, and 2 splits as (1^3) in k.

$$\Phi_k(s) = \left(1 + \frac{1}{2^s} + \frac{2}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2} \left(1 + \frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2} \left(1 + \frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{3}{p^s}\right).$$

- k defined by $x^3 - 4x - 1 = 0$, $\mathrm{Disc}(k) = 229$, $\mathrm{rk}_2^+(k) = 1$, and 2 splits as (21) in k.

$$\begin{aligned}\Phi_k(s) = {} & \left(1 + \frac{1}{2^{2s}} + \frac{4}{2^{3s}} + \frac{2}{2^{4s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2,\ p\neq 2} \left(1 + \frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2} \left(1 + \frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{3}{p^s}\right) \\ & + \left(1 - \frac{1}{2^{2s}}\right) \prod_p \left(1 + \frac{\omega_L(p)}{p^s}\right),\end{aligned} \tag{8.8}$$

where L is the S_4-quartic field of discriminant $64 \cdot 229$ defined by $x^4 - 2x^3 - 4x^2 + 4x + 2 = 0$.

10.3 Examples with signature conditions

Finally, we work out examples of the series $\Phi_k^+(s)$, described in Section 9, in both the S_4 and A_4 cases.

- k noncyclic cubic defined by $x^3 - x^2 - 5x + 4 = 0$, $\mathrm{Disc}(k) = 469$, where 2 splits as (21).

$$\begin{aligned}\Phi_k^+(s) = \frac{1}{4}\Bigg(&\left(1+\frac{1}{2^{2s}}+\frac{4}{2^{3s}}+\frac{2}{2^{4s}}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2,\ p\neq 2}\left(1+\frac{1}{p^s}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1^2\mathfrak{p}_2,\ p\neq 2}\left(1+\frac{1}{p^s}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2}\left(1+\frac{3}{p^s}\right)\\ &+\left(1+\frac{1}{2^{2s}}-\frac{4}{2^{3s}}+\frac{2}{2^{4s}}\right)\prod_{\mathfrak{p}\neq 2}\left(1+\frac{\omega_{L_1}(p)}{p^s}\right)\\ &+\left(1-\frac{1}{2^{2s}}\right)\prod_{\mathfrak{p}\neq 2}\left(1+\frac{\omega_{L_2}(p)}{p^s}\right)+\left(1-\frac{1}{2^{2s}}\right)\prod_{\mathfrak{p}\neq 2}\left(1+\frac{\omega_{L_3}(p)}{p^s}\right)\Bigg).\end{aligned}$$

  In the above, we have $|C_{(4)}^+| = 4|C_{(1)}^+| = 4$, and there are three fields L_1, L_2, L_3 in $\mathcal{L}_2^*(k)$, of discriminants $(-1)^2 2^4 \cdot 469$, $(-1)^2 2^6 \cdot 469$, and $(-1)^2 2^6 \cdot 469$ respectively, where $(-1)^2$ indicates that each field has two pairs of complex embeddings, and in which the splitting of 2 is respectively (2^2), (1^4), and (1^4). The total of the 2-adic factors is $1 + 2^{-4s}$, corresponding to the fact that the only totally real quartic field of discriminant $2^a \cdot 469$ is $\mathbb{Q}(x)/(x^4 - 14x^2 - 4x + 38)$, of discriminant $2^4 \cdot 469$.

- An example where $|C_{(4)}^+| = 2|C_{(1)}^+|$ is furnished by $k := \mathbb{Q}(x)/(x^3 - 4x - 1)$, the unique cubic field of discriminant 229. We again have three fields in $\mathcal{L}_2^*(k)$, with discriminants $(-1)^2 229$, $(-1)^0 2^6 229$, and $(-1)^2 2^6 229$. Again $\Phi_k^+(s)$ is a sum of four terms which can be written down as in the previous example.
- An A_4 example: k cyclic of discriminant 31^2, defined by $x^3 - x^2 - 10x + 8 = 0$, in which 2 is totally split.

$$\begin{aligned}\Phi_k^+(s) = \frac{1}{4}\Bigg(&\frac{1}{3}\left(1+\frac{3}{2^{2s}}+\frac{6}{2^{3s}}+\frac{6}{2^{4s}}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}\left(1+\frac{3}{p^s}\right)\\ &+\left(1-\frac{1}{2^{2s}}+\frac{2}{2^{3s}}-\frac{2}{2^{4s}}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}\left(1+\frac{\omega_L(p)}{p^s}\right)\Bigg).\end{aligned}$$

Acknowledgments

The authors would like to thank Karim Belabas, Darrin Doud, Arnaud Jehanne, Franz Lemmermeyer, Guillermo Mantilla-Soler, Jacques Martinet, and Simon Rubinstein-Salzedo, among many others, for helpful discussions related to the topics of this paper.

Thorne's work is partially supported by the National Science Foundation under Grant No. DMS-1201330.

Author details

[1] Université de Bordeaux, Institut de Mathématiques, U.M.R. 5251 du C.N.R.S, 351 Cours de la Libération, 33405 Talence Cedex, France. [2] Department of Mathematics, University of South Carolina, 1523 Greene Street, Columbia, SC 29208, USA.

Received: 12 March 2015 Accepted: 13 March 2015
Published online: 04 October 2016

References

1. Armitage, J, Fröhlich A: Class numbers and unit signatures. Mathematika **14**, 94–98 (1967)
2. Baily, A: On the density of discriminants of quartic fields. J. Reine Angew. Math. **315**, 190–210 (1980)

3. Bhargava, M: Higher composition laws II: On cubic analogues of Gauss composition. Ann. Math. **159**(2), no. 2, 865–886 (2004)
4. Bhargava, M: Higher composition laws III: The parametrization of quartic rings. Ann. Math. **159**(3), no. 3, 1329–1360 (2004)
5. Bhargava, M: The density of discriminants of quartic rings and fields. Ann. Math. **162**(2), no. 2, 1031–1063 (2005)
6. Cohen, H: Advanced topics in computational number theory. Graduate Texts in Math, Vol. 193. Springer-Verlag, New York (1999)
7. Cohen, H: Counting A_4 and S_4 number fields with given resolvent cubic. Proc. Banff Conf. Honor Hugh Williams, Fields Inst. Comm. **41**, 159–168 (2004)
8. Cohen, H, Diaz y, Diaz, F, Olivier M: Counting cyclic quartic extensions of a number field. J. Th. Nombres Bordeaux **17**, 475–510 (2005)
9. Cohen, H, Diaz y, Diaz, F, Olivier M: Enumerating quartic dihedral extensions of $\mathbb{Q}$. Compositio Math. **133**, 65–93 (2002)
10. Cohen, H, Diaz y, Diaz, F, Olivier, M: Counting biquadratic extensions of a number field. preprint
11. Cohen, H, Diaz y, Diaz, F, Olivier M: Counting discriminants of number fields. J. Th. Nombres Bordeaux **18**, 573–593 (2006)
12. Cohen, H, Diaz y, Diaz, F, Olivier, M: Counting A_4 and S_4 extensions of number fields. unpublished preprint
13. Cohen, H, Morra, A: Counting cubic extensions with given quadratic resolvent. J. Algebra **325**, 461–478 (2011). (Theorem numbers refer to the published version, which are different than in the arXiv version.)
14. Cohen, H, Thorne, F: Dirichlet series associated to cubic fields with given quadratic resolvent. Michigan Math. J. **63**(2), 253–273 (2014)
15. Cohen, H, Rubinstein-Salzedo, S, Thorne, F: Identities for field extensions generalizing the Ohno-Nakagawa relations. Compos. Math. **151**(11), 2059–2075 (2015)
16. Cohn, H: The density of abelian cubic fields. Proc. Amer. Math. Soc. **5**, 476–477 (1954)
17. Dribin, DM: Quartic fields with the symmetric group. Ann. of Math. **38**(2), no. 3, 739–749 (1937)
18. Hasse, H: Number theory. Springer-Verlag, Berlin (2002)
19. Heilbronn, H: On the 2-classgroup of cubic fields. Studies in Pure Mathematics (Presented to Richard Rado). pp. 117–119. Academic Press, London (1971)
20. Jehanne, A: Réalisation sur $\mathbb{Q}$ de corps de degrés 6 et 8. PhD thesis, Université Bordeaux I (1993)
21. Jones, J, Roberts, D: A database of local fields. J. Symbolic Comput. **41**, no. 1, 80–97 (2006). accompanying database available online at, http://math.asu.edu/jj/localfields/
22. Jones, J, Roberts, D: A database of number fields. LMS J. Comput. Math. **17**(1), 595–618 (2014). Accompanying database available online at http://hobbes.la.asu.edu/NFDB/
23. Nakagawa, J: On the relations among the class numbers of binary cubic forms. Invent. Math. **134**, no. 1, 101–138 (1998)
24. Ohno, Y: A conjecture on coincidence among the zeta functions associated with the space of binary cubic forms. Amer. J. Math. **119**, no. 5, 1083–1094 (1997)
25. The PARI Group: PARI/GP version 2.8.0, Bordeaux (2015). http://pari.math.u-bordeaux.fr/
26. The PARI Group, Voight, J, Jones, J, Roberts, D, Klüners, J, Malle, G: *Global number fields*. Online databases available at http://www.lmfdb.org/NumberField/ and http://pari.math.u-bordeaux.fr/pub/numberfields/
27. Scholz, A: Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. J. Reine Angew. Math. **166**, 201–203 (1932)
28. Wood, MM: On the probabilities of local behaviors in abelian field extensions. Compositio Math. **146**, 102–128 (2010)
29. Wong, S: Arithmetic of octahedral sextics. J. Number Theory **145**, 245–272 (2014)
30. Wright, DJ: Distribution of discriminants of abelian extensions. Proc. London Math. Soc. **58**(3), 17–50 (1989)
31. Wright, DJ: Yukie A: Prehomogeneous vector spaces and field extensions. Invent. Math. **110**, 283–314 (1992)